Best Practices for Accounts Payable Course Instructions

Author: Mary Schaeffer

NASBA - Sponsor number: 103021

Wolters Kluwer, CCH is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors. State Boards of Accountancy have the final authority on the acceptance of individual course for CPE credit. Complaints regarding registered sponsors may be submitted to the National Registry of CPE Sponsors through its website: www.nasbaregistry.org.

Instructions to Participants

To assist the participant with navigating the learning process through to successful completion, this course has been produced with the following elements:

Overview of Topics / Table of Contents: This serves as your overview of topics for the program.

Definition of Key Terms / Glossary: You'll find key terms defined for this program in the course materials.

Index / Key Word Search: This course contains a traditional index with page numbers referenced for each topic. You can also find information quickly in the PDF materials by using the search function built into your Adobe Reader.

Review Questions: Questions that test your understanding of the material are placed at the end of each learning activity throughout the course. Explanatory feedback for each incorrect answer, and reinforcement feedback for the correct answer for the review questions are placed at the end of the book.

Final Exam: The final exam measures if you have gained the knowledge, skills, or abilities outlined in the learning objectives. We recommend you print out the final exam questions to reference as you go through the material. You may submit your final exam for online grading at any time. Exams are graded instantly. You are allowed three attempts to pass the final exam. A minimum score of % is required to receive the certificate of completion. **You have one year from date of purchase to complete the course.**

Course Evaluation: Once you have successfully passed your online exam, please complete our online course evaluation. Your feedback helps Wolters Kluwer maintain its high quality standards!

About This Course

This section provides information that is important for understanding the course, such as course level and prerequisites. Please consider this information when filling out your evaluation after completing the course.

Publication Date: May 2019

Course Description
Best practices for the accounts payable function are critical for those organizations concerned about their profitability. For poor practices result in excess cost, duplicate payments, increased processing expenses, fraud and frayed vendor relationships. And, of course there is the growing issue of regulatory compliance as the Feds and states look for their fair share.

This course presents information the professional can use to identify best practice problems as well as regulatory concerns. Industry expert Mary S. Schaeffer explains the issues related to the accounts payable function to auditors, controllers, and managers. She then reveals the best practices for a myriad of these issues as well as identifying almost best practices for those cases where it is not possible to use the best practice and the worst practices which are likely to cause trouble.

Learning Objectives
Upon successful completion of this course, participants should be able to:

- Recognize how to establish strong master vendor file practices
- Identify how to incorporate appropriate segregation of duties into master vendor file process
- Describe how to create effective invoice receipt practices
- Recognize how to construct best practice invoice handling routines
- Describe effective practices when short-paying invoices
- Identify how to establish a process for managing discrepant invoices
- Recognize and implement a suitable process for storing check stock
- Identify the benefit of paying electronically
- Describe a process to weed out fraudulent change of bank account requests
- Recognize how to develop strong controls in a p-card program
- Identify ways to pay small dollar invoices without issuing a check
- Identify lost funds through an effective supplier statement review policy
- Recognize how to integrate the concept of segregation of duties across the payment process
- Recognize how to cncover practices that will eliminate weak control points
- Identify the importance of having a separate computer for online banking
- Recognize how to integrate check fraud prevention practices into the accounts payable process
- Identify how to create a strong travel and entertainment policy the is compliant with IRS guidelines for the entire organizations
- Identify how to develop policies for handling travel issues created when employees leave
- Identify what is required for information reporting to the IRS for independent

contractors
- Describe how to integrate use of IRS TIN Matching into the new vendor setup function
- Describe how to create a policy that will enable the organization to report and remit unclaimed property in all instances
- Recognize how to incorporate regular OFAC checking into the payment process to ensure payments are not made to terrorists
- Identify potential situations where a payment may actually be a bribe to a foreign official in conflict with FCPA regulations
- Identify how payment timing can both help and hurt the organization
- Recognize how to create procedures to ensure all early payment discounts are earned

NASBA Field of Study
Accounting. Some state boards may count credits under different categories—check with your state board for more information.

Course Level
Overview. Program knowledge level that provides a general review of a subject area from a broad perspective. These programs may be appropriate for professionals at all organizational levels.

Prerequisites
None.

Advance Preparation
None.

Course Expiration
AICPA and NASBA Standards require all Self-Study courses to be completed and the final exam submitted within 1 year from the date of purchase as shown on your invoice. No extensions are allowed under AICPA/NASBA rules.

Contributors

Technical Review: Kelen Camehl

Table of Contents

Introduction

The accounts payable function has changed a lot in the last five years. As the cost of technology plummets, new and more effective applications are being written for the accounts payable function. In fact, accounts payable is the leading application on list of accounting areas likely to be impacted by artificial intelligence (AI).

In the last few years we've also seen a blurring of the lines between what we used personally and what is appropriate for business. Sites such as LinkedIn and Facebook (yes, Facebook) are mostly thought of in the realm of personal business. But savvy professionals have found ways to use both to run a more efficient accounts payable function. Today, most job listings for professionals are listed on LinkedIn, although that is not the only way LinkedIn can be used to run a more efficient accounts payable function.

The course analyzes the processes used in the accounts payable function. Each of the issues is explained and a best practice identified. More than occasionally, the best practice has several components so the explanations make take a few paragraphs.

Recognizing that for a variety of reasons, an organization might not choose to or be able to utilize the preferred practice, the applicable second choice, the almost best practice is pinpointed. In some cases, there are none. There is only one right way to handle the particular issue.

Before homing in and identifying all the worst practices associated with a particular issue, we home in on special pointers to help those managing the accounts payable function. These are items that might not be obvious at first glance. The pointers also include some caveats and/or problems some might run into.

The work starts with a look at the accounts payable function and recommended practices to use when managing the function. It then moves on to what I believe should be the first step in the procure-to-pay practice, the master vendor file. Since we're talking about a best practice world, we can assume the vendor will be set up in the master vendor file before the first purchase order is written, although that happens in only a minority of the cases.

After the master vendor file, this course has two chapters on invoice processing and invoice problems. It then looks at the end of the procure-to-pay process, the payment side. This includes chapters on paying by check, electronic payments, and p-cards. It also examines several practices related to establishing an overall payment strategy, which every organization should do.

At that point, the course veers into a look at some of the background issues related to the accounts payable function. Despite the fact that they are not the ones that come immediately to mind when accounts payable is mentioned, handling them properly can mean operating a leading-edge best practice operation while ignoring them can lead to duplicate payments, fraud, IRS problems and other unpleasant outcomes.

The course has one chapter devoted exclusively to the policy and procedures manual, an often-overlooked issue. It then delves into the operational aspects of accounts payable, a look at reducing duplicate payments and establishing strong internal controls.

Although we could have devoted a whole course to payment fraud, this was not the place for that and two chapters focus in on best practices that will help any organization prevent and detect fraud.

No course on best practices would be complete without an examination of regulatory issues. So, we investigate best practices related to information reporting, 1099s, unclaimed property, sales and use tax reporting and remitting, OFAC checking, and FCPA compliance.

One of the areas that has experienced the most change is the way we use technology in accounts payable. The chapter on this issue delves into invoice automation, electronic invoicing, use of mobile devices (smartphones and tablets) and establishing an overall technology strategy for the accounts payable function.

Just because we rely on technology does not mean that communicating with vendors is still not critical. It is and we discuss several ways to disseminate information to them. And finally, we close with a look at cash flow issues. Accounts payable no longer operates as its own little silo. It is an integral part of the accounting and finance chain and as such, its impact on cash flow is discussed.

It's a whole new playing field, and to be successful, all organizations need to employ as many best practices as possible; for by their very nature best practices incorporate strong internal controls. What follows is a look at the various functions that make up accounts payable and the best practices associated with each.

¶100 Managing the AP Function

Learning Objectives

Upon completion of this chapter, you will be able to:

Implement a best practice policy

Utilize a policy and procedures manual effectively

When it comes to running an efficient accounts payable function, policies and procedures need to be set at the top, with the staff following directives and policies set by management. In this chapter, we will discuss:

Reasons Why Best Practices Matter
Best Practice Policy
Policy and Procedures Manual
Staff Training
Soliciting Process Improvement Recommendations
Payment Audits

¶101 Ten Reasons Why Best Practices in Accounts Payable Matter

Before we delve into the 101 best practices, we thought it might be a good idea to examine just why best practices are so important. From time to time, most people who work in accounts payable run into a smart-aleck who demands to know "what's the big deal about accounts payable?" These folks think that an effective accounts payable process is one where someone sits at a desk and simply writes checks for any invoice that crosses their desk. As those who work in the function know only too well, this practice would be a recipe for disaster. Here's a look at what could go wrong should an organization be foolish enough to follow such a practice.

Reason #10: The organization would end up paying invoices twice. This is because some vendors send invoices twice as a matter of practice (e-mail and postal mail) while others only send that second invoice when a payment is later. Whatever the reason for the sending of the second invoice, an organization not employing best practices and strong internal controls would result in duplicate payments—which vendors rarely return unless asked.

Reason #9: The organization would be hit with more fraud. Once crooks realized that the organization was paying whatever invoices came its way, the less than honest ones would start sending double and triple invoices and perhaps even some for goods and services not purchased.

Reason #8: As long as the organization was not concerned about the bottom line (and virtually all are!), ignoring best practices would be fine. For duplicate invoices and other excess expenses come right off the bottom line, impacting the profitability of the organization in a negative manner.

Reason #7: When best practices are not followed, payments are typically delayed. This does not sit well with vendors. Typically, when payments are delayed, vendors have a difficult time getting a straight answer as to when they can expect their payments. None of this is conducive to strong relations, and hence vendor relations tend to be damaged.

Reason #6: While best practices result in an efficient accounts payable function, the reverse is true when best practices are ignored. The end result is that additional staff will be needed to handle the same amount of work.

Reason #5: It will come as no surprise to those reading this to learn that inefficient processes lead to increased expense for the accounts payable function. This may come in the form of extra staff, lost early payment discounts, or late fees.
Reason #4: While most would like to forget about the Sarbanes-Oxley Act, those in the public arena don't have that luxury. Since best practices go hand-in-hand with strong internal controls, no public company can afford to ignore the issue of best practices. It should also be noted that some private companies are subject to the requirements of Sarbanes-Oxley either because their lenders demand it or a large customer will only do business with organizations that are SOX compliant.
Reason #3: Often, not employing best practices results in inaccurate information that trickles down to the financial statements, resulting in inaccurate financial statements. This is a worst-case scenario and one that every organization should strive to avoid. It can also mean being singled out by auditors (internal or external) for financial statement issues. This is not an area where most accounts payable departments have any interest in being mentioned, and most strive to avoid it.
Reason #2: Inaccurate financial statements and financial reporting can lead to trouble for executives relying on faulty financial information for business decisions. Use of best practices in the accounts payable arena can lead to improved forecasting, especially when it comes to cash flow.
Reason #1: If everything discussed so far has not been enough to convince you that best practices are a necessity, consider the following. By not using best practices across the entire accounts payable function, you could be courting trouble with the IRS and state taxing authorities. For example, many believe that under-reporting of income by independent contractors and other self-employed individuals is largely responsible for the tax gap. The attention on this issue is focused on the corporate world for sometimes questionable practices when it comes to 1099 reporting.

Along the same lines, many believe that only one-third of all organizations that should be reporting and remitting unclaimed property are actually doing so. The result is that many organizations are wide open for trouble in this regard. And, you don't have to go far to find a story bewailing online sales on the Internet and their impact on the states' collection of sales and use tax.

Given these issues and others, it is imperative that all organizations look at their accounts payable function and employ as many best practices as they can integrate across the entire cycle.

¶102 Best Practice Policy

Best practices are no longer set in stone. What worked yesterday may not work today or tomorrow. What's more, there have been a few instances where worst practices have turned into best practices. Automation, increased regulatory pressures, and a relentless push for efficiency across the corporate spectrum have taken their toll. It is no longer possible to establish best practices and set the accounts payable wheels in motion and then forget about the process. Those days are gone.
Best Practice: Regularly review the practices used in your accounts payable function. Keep up-to-date on the latest changes. As you note where process improvements could be made, update your procedures and train everyone affected by the change. What's more, if you note a series of mistakes that require a process change in order to eliminate that error, make that improvement immediately. Once you've made the change, reflect it in your accounts payable policy and procedures manual and make sure everyone on staff is trained in the new methodology.
Almost Best Practice: Some organizations find it difficult to implement the type of continuous improvement cycle described above. For these firms, a once a year review and overhaul is the next best bet. Of course, this should be followed by updating the policy and procedures manual and retraining of the staff, should any changes be made. It is also possible that you'll do the annual review and from time to time, no changes will be required. However, don't count on that and skip the annual review. For if you skip it for a few years in a row, you are apt to find your processes are woefully out-of-date.
Special Pointers for Accounts Payable: It is imperative that any time you make a change to your practices, be it once a year or on an ongoing basis, everyone on staff is trained and all start using the new process at the exact same point. For if one does it one way and a second processor a different way, the odds of introducing errors and duplicate payments skyrocket.

Worst Practice: Not regularly reviewing and updating your practices to reflect current thinking related to best practices. For if there is no regular review, and you stick with the practices used in the past, before you know it your accounts payable function will be woefully out of date. This may mean missing a regulatory compliance issue that could get your company into hot water with the states or the feds or duplicate payments, or increased likelihood of fraud.

¶103 Policy and Procedures Manual

The accounts payable policy and procedures manual should be the core document for the accounts payable department. It should document in detail the processes used within the department. Some refer to it as the bible for accounts payable. Having an updated accurate policy and procedures manual can come in handy if you are subject to an information reporting audit, a sales tax audit, or an unclaimed property audit.

By being able to show documentation that demonstrates your good intent when it comes to these regulatory issues, you may be able to have fines or penalties abated. However, if the manual documents procedures that are not consistent with the law, the manual will not help you. A simple example might be if your policy and procedures manual shows that you routinely write off uncashed checks to miscellaneous income instead of reporting and remitting them to the states. In this case your documentation would not show good intent and would not help you.

Best Practice: Any time you make a change in your processes, the manual should be immediately updated. Copies of the updated manual should be shared with all who are affected by the change or might need to know about it. Since these manuals are no longer printed but are usually a Word document saved as a PDF file, it is relatively easy to update and share—and there is no cost associated with printing new manuals. If no change has been made within the last 12 months, a quick annual review is a good idea.

Almost Best Practice: If it is not possible to continually update the manual, save all changes for an annual review and update. Then, all recommended changes that came to light within the last year can be incorporated in one big update.

Special Pointers for Accounts Payable: The manual should not be a static document, but rather one that is used on a regular basis. Updated copies should be given to the existing staff to be used as a reference guide. This is particularly important if your accounts payable staff handles certain functions once or twice a year and may forget the details in the interim. They can turn to the manual instead of bothering the manager for the information they need. In fact, the staff should be encouraged to use the manual and only come to the manager if they can't find the answer in the manual.

Worst Practice: As you might expect, the worst practice regarding the accounts payable policy and procedures manual is creating a manual and then putting it on the shelf, never updating it or using it as a reference guide. This is a complete waste of time and effort. From time to time, I am asked by those without a current manual if they can buy one or simply download one off the Internet. While each of these approaches is possible, they won't give you a manual that reflects your current operations. They will require extensive review and editing. If you take someone else's manual, you get someone else's policies and procedures, which probably don't reflect what is going on in your shop.

¶104 Staff Training

Keeping the staff up-to-date on changing best practices, changing regulatory requirements, and new technology affecting accounts payable is not an easy task. This is on top of training the staff on the particulars of their day-to-day assignment. Unfortunately, due to the recent harsh recession, many organizations have cut training budgets to the bone. This has resulted in training falling to the already overworked manager and often just being skipped completely, with the idea that the organization will include training in next year's budget, or perhaps the following year. Given the pace of change in the business world, no organization can afford to skimp on training. But, that's exactly what has happened.

Best Practice: Budget for ongoing training for every single member of the staff. If this is not possible, take the do-it-yourself approach. Assign each staff member a topic for which they are to become the resident subject matter expert. Make them responsible for periodic updates at staff meetings. Even if it is not possible

to send the entire team for training, if one person goes, that person should be charged with updating his or her colleagues when they return from the event.

Almost Best Practice: Whether the organization has a budget for training or not, there are many low-cost or no-cost opportunities available. Many vendors offer free webinars with a demonstration of their product at the end. Some complain about these product demos, but I think they are missing the big picture. First, the product demo comes at the end, so if it is an online event, you can simply log out. But a better approach is to stay and listen to the product demo. This is a great way to learn what's on the market without having to deal with an aggressive salesperson in your office. You can devote as much or as little time to these presentations without worrying about offending the salesperson. Don't overlook free electronic news alerts, from vendors and professional associations.

Special Pointers for Accounts Payable: Attend as many of the vendor webinars described above so you will be conversant about new products on the market. You'll begin to see which ones would work best for your organization and which ones have features that your organization is not likely to use. One last point for accounts payable: If you see an event (or a subscription) that you think would benefit your organization if you were to attend, prepare a proposal for your boss. List the benefits for the company—not for you. You can get these by reviewing the list of topics and sessions to be covered at the event.

Worst Practice: Doing nothing because you either don't have budget or don't think management would approve the expenditure for training. There's a lot you can do on your own to keep up, so there's no reason not to. And finally, if you ask to attend a particular function or event, the worst that can happen is your manager will say no. Then you are in exactly the same position as if you didn't ask. And, you may be pleasantly surprised.

¶105 Soliciting Process Improvement Recommendations

Many organizations overlook their very best source of process improvement recommendations: the staff who handles the particular function. This is just as true in accounts payable as it is in other functions throughout the organization.

Best Practice: Process improvement suggestions can come from a variety of places. But, an often overlooked source is the folks who handle the day-to-day work. They are the most knowledgeable when it comes to how the task is done. They can tell you where you can make changes and where the changes you might want to make will not work. While asking the staff for process improvement recommendations is a good idea, it has to be done with care. Sometimes the suggestions offered by the staff will make the accounts payable function more efficient but will result in problems elsewhere in the accounting chain. Thus it is imperative that the changes proposed be thoroughly analyzed. Then, if the recommendation is a good one, the change needs to be made across the board, with everyone doing the same function making the change.

Almost Best Practice: After you've gone through all the recommendations made by the staff you might want to sit with several processors and watch them go through their work, seeing if you can identify additional points where the process might be able to be improved. This task can be done either by the manager or a consultant or an analyst who works with the staff. Whatever suggestions arise from this exercise need to be vetted by the staff to make sure they are feasible and by a manager to ensure there are no problems created for others working with the information.

Special Pointers for Accounts Payable: Should any of the process improvement suggestions be adopted, they need to be incorporated in the policy and procedures manual. The entire staff needs to be trained using the new process as all should start using it at the same point. If some of the recommendations get turned down, don't take it personally. Remember, there's a big picture and the suggestion must be good for everyone, not just accounts payable.

Worst Practice: Similar to the previous discussion about not updating policies and procedures, going along using the same processes for year after year without taking the time out to review existing procedures to see if they still make sense and result in an efficient accounts payable function. At a bare minimum, review what you are doing once a year to see if any changes are required.

¶106 Payment Audits

The issue of payment audits can cause heated debate among professionals in accounts payable. Only about one in three organizations have one of these audits done on a regular basis. A payment audit involves a third-party firm reviewing the payment activity with an eye towards identifying and recovering duplicate and erroneous payments. These audits typically also involve the third party recovering unidentified open credits.

There are many benefits associated with having a payment audit done. Clearly there is the financial gain of the funds recovered during the audit. These are reduced by the contingency percentage typically taken by the audit firm. Additionally, the firm should prepare a management report highlighting any weaknesses in your existing process. This report should be scoured thoroughly and the weak spots identified should be fixed.

Too often people boast that the reason they don't have an audit done is they never make a duplicate payment. Unfortunately, even the best-run organization makes a mistake from time to time. What's more, if the person is correct and no duplicate payments are ever made, then the cost for the audit will be minimal, assuming an agency working on a contingency basis is selected.

Another reason people sometimes give for not having an audit done is the expense. They claim the firms charge too much. Let's look at a simple example and see if that theory holds water. Let's assume the audit firm finds and recovers $1 million for the client. In this hypothetical case, the audit firm gets a 25 percent contingency fee, leaving the client with $750,000 of the $1 million. But, if the firm is not hired, how much will the client recover? How much does it cost not to hire the audit firm? If you are saying nothing, I do not agree. I believe it cost the client $750,000 that will never be recovered unless an audit firm is hired.

This brings up one last issue, or dirty little secret, related to recovery audits. Many people have asked, "Well, doesn't the vendor return duplicate payments?" And the answer to that question is "most don't." About 1 in 100 vendors will return a duplicate payment without any prompting. The next issue raised is about unclaimed property. And, the answer is yes, the vendor should be turning this money over to the states as part of its unclaimed property reporting—three, four, or five years later. However, most don't. They either write it off to miscellaneous income or use it to cover unearned early payment discounts, unauthorized deductions or discrepant invoices. At the end of the day, unless you hire a third-party firm or set up a separate unit to recover duplicate and erroneous payments, most of your money held with vendors will be lost.

Best Practice: As suggested above, you can do some easy processes to strip off the low-hanging fruit in terms of duplicate and erroneous payments and open vendor credits. If you have adequate staff, you can request quarterly statements from vendors and recover open credits yourself. Once you've done everything you possibly can, call in the pros and see what they can find. Ideally this should be an ongoing process so the vendors don't have a chance to "use" your open credits to clean up their books.

Almost Best Practice: If you don't have the resources to have a continual audit, try and do it once a year. This is one area where best practices have changed radically. We used to recommend once every two years, but that no longer seems adequate.

Special Pointers for Accounts Payable: Many accounts payable departments are reluctant to have a payment audit done for fear they will be blamed for any funds recovered by the audit firm. This is not fair for often the errors are a result of poor practices elsewhere in the procure-to-pay chain. By getting the management report, you will be able to identify these problems. Accounts payable can also make sure that vendors send credit memos directly to accounts payable. Too often they go to purchasing staff, who then throws them away or files them, not realizing what they are.

Finally, there is the unclaimed property issue. As mentioned above, these items should be turned over to the state and sometimes they are. In fact, audit firms know that they can start their recovery by reclaiming funds turned over to the state. This is something you can do yourself, assuming you are currently reporting and remitting your organization's unclaimed property. If you are not, filing a claim is like waving a red flag in front of a bull. It will trigger an audit. The amount you recover will be small in comparison to the pain and cost of an audit, when you are not in compliance. Of course, the best practice advice in this arena is to

get in compliance. This issue should be kept in mind when hiring the audit firm. If you don't want them recovering funds from the state, tell them this is *not* to be part of the audit.
Worst Practice: Not having an audit done because you believe you "never make a duplicate payment."

Review Questions

1. When best practices are ignored, which of the following is likely to happen?
   a. The AP manager will be promoted.
   b. Duplicate payments are more apt to occur.
   c. The opportunity for fraud decreases.
   d. Financial statements are apt to be more accurate.

2. Which of the following is likely to occur when best practices are not followed?
   a. Regulatory problems increase.
   b. Regulatory problems decrease.
   c. There is no effect on regulatory issues.
   d. Regulatory pressures disappear.

3. Which of the following is a best practice when it comes to establishing a best practice policy for the accounts payable function?
   a. Update the policy whenever a change is made.
   b. Review the policy once a year and update it for all changes made during the year.
   c. Never review the policy; once it's set, it's good for life.
   d. You don't need a policy if there are sufficient internal controls.

4. Who should have a copy of the policy and procedures manual?
   a. Only the AP manager
   b. Only supervisors and managers
   c. Only invoice processors
   d. Anyone who needs to see it

5. Which of the following is a reasonable approach when there is little budget training?
   a. Forget about staff training and hope there will be budget next year.
   b. Make staff responsible for their own staff training.
   c. Bring in an expert and charge each staff member for a portion of their fees.
   d. Assign topics and encourage each staff member to find information on the Internet and then share their intelligence with the rest of the staff.

¶200 Master Vendor File

Learning Objectives

Upon completion of this chapter, you will be able to:

Establish strong master vendor file practices

Incorporate appropriate segregation of duties into master vendor file process

Create reasonable master vendor file cleanup practices

The master vendor file is critical in the operation of an accounts payable function. When overlooked, poor practices lead to weakened internal controls, potential duplicate payments, and the increased possibility of fraud, especially internal fraud. In this chapter, we cover the following:

Who Has Access to the Master Vendor File?
Master Vendor File Setup
Naming Conventions
Updating the Master Vendor File
Master Vendor File Cleanup
Self-Service Master Vendor Files

¶201 Who Has Access to the Master Vendor File

While it is definitely easier for the staff processing invoices for payment if they can add vendors to the master vendor file whenever they get an invoice from a new vendor, that practice is an invitation to trouble. Unfortunately, that's how a number of organizations handle putting information into the master vendor file. This means giving access to the master vendor file to a large number of individuals. This is a terrible idea. It completely disregards the best practice concept inherent in all accounting functions of having appropriate segregation of duties.

Best Practice: Access to the master vendor file, for anything but information lookup, should be severely limited. Only a few people should be able to enter information, be it for setup or to make changes. The employees with this access should not perform any other tasks in the procure-to-pay function, making it more difficult for someone to defraud the organization. What's more, when they go on vacation, their passwords and access should not be given to someone else. This will simply muddy the audit trail should there be a problem down the line. A better approach is to set up the backup person with their own user ID and password and then deactivate those when the person with primary responsibility for the task returns. This is less of a problem in large organizations where there will be several people working on the master vendor file.

Almost Best Practice: This is a black-and-white issue, so there really is no almost best practice. In many organizations there are one or two people with access to the entire accounts payable function. Typically this is the manager, director, or perhaps the controller. While this is not a good idea, it does solve the problem of an unexpected absence, assuming the person with the broad access is willing to dive in and handle the task. Really, though, unlimited access is not a good idea.

Pointer for Accounts Payable: While limiting access for the purposes of adding new vendors or updating information on existing vendors can seem to make the accounts payable function run less smoothly, it is imperative from an internal control standpoint. Sometimes what is easier for accounts payable is not necessarily good for the organization as a whole, and this is one of those instances.

Worst Practices: Worst practices include:

Letting each processor update information about their own vendors
Letting each processor add vendors whenever it seems necessary

¶202 Master Vendor File Setup

Setting up the master vendor file is one of those functions that no one really focuses on too much. However, handled ineffectually, it can and does lead to duplicate payments and opens the door to fraud. It contains the vital information about a company's vendors. The data contained in each master vendor file will vary from industry to industry. Usually the responsibility for setting up vendors and maintaining them in the master vendor file resides in accounts payable. Sometimes it is in purchasing. Occasionally, each department has its own master vendor file, although this is generally not recommended.

Best Practice: The function should be handled by the organization that can best achieve appropriate segregation of duties. If the staff is small in accounts payable and in purchasing, this might mean the responsibility should reside elsewhere in the accounting function. Vendors should be set up on the master vendor file before any payments are made. Most companies only set up companies if they believe there will be an ongoing relationship with that firm. One-time transactions are typically not set up in the master vendor file, although a sizeable minority does set them up. Information included in the files might include:

- Vendor Name (legal)
- DBA (Doing Business As)
- Business Address
- Ship to Address
- Remit to Address
- Bill to Address (including a contact name)
- Phone Number
- Fax Number
- EIN (Employer Identification Number)
- Form W-9 (on file) Yes/No
- TIN (Tax Payer Identification Number) Matching Success Yes/No
- For (Electronic Funds Transfer) EFT Payments:
  - Name on Bank Account
  - Bank's Routing Number
  - Bank Account Number
  - Bank's ACH (Automated Clearing House) contact
  - Bank's Contact Phone Number
  - Type of Business
  - Incorporated
  - AR Contact Name, E-Mail Address, and Phone Number

A form can be used to accumulate this data. Once the information has been compiled, authorized parities should approve (i.e., sign) it.

While most people believe the function belongs in accounts payable, especially when many independent contractors are used, it is acceptable to have it in purchasing, assuming all the rules are followed. Ideally, there should be only one master vendor file.

Each vendor should have one, and only one, master vendor file. When a vendor has several, the door for duplicate payments is swung wide open.

A strict naming convention should be adhered to when setting up master vendor files. While at first glance this may seem silly, there are very good reasons for it. For example, a company called The Purple Cafe could be set up as any one of the following:

- The Purple Cafe
- Purple Cafe, The
- Purple Cafe

There is no right or wrong way to set it up—just as long as the leading "The" is always treated in the same manner. Similarly, let's look at IBM to see what could go wrong. Here are a few ways the venerable computer company could be listed:

IBM
I B M
I.B.M.
International Business Machine

Without a naming convention, several files could be set up for the same company. This also makes it difficult for accounts payable associates checking the master vendor file to ascertain if a payment has been made. Which IBM file should they look in?

Here are some guidelines you might use:

Use the initials or acronym rather than the full name of vendors commonly known by their initials or an acronym (i.e., IBM, not International Business Machine).

Do not use abbreviations except as above (i.e., Olympia & York, not O & Y).

Use an & for vendors with the word *and* in their name (i.e., D&H, not D and H).

Eliminate spaces and period between initials (i.e., IBM, not I B M or I.B.M.).

For individuals, use their first name then a space then their last name (i.e., Mary Schaeffer, not Schaeffer, Mary or Schaeffer Mary).

Do not leave a space between Mc (or Mac) in either a company or individual's name (i.e., MacDonald, not Mac Donald).

Companies typically assign a vendor number to each vendor. Companies also typically include their employees who travel in their vendor files. This is so travel and entertainment (T&E) reimbursement payments can be made. Some use the employees' social security number as the employee ID number and in the master vendor file. With all the recent problems with identity theft, this once common practice should be eliminated. Employees who regularly receive payments should be assigned a vendor number that is different than the social security number. In fact, some question whether it is necessary to have this information for employees in the vendor file.

As it is often difficult to get W-9 information from independent contractors, making a completed W-9 form part of the process of setting up the master vendor file is a good idea. Without the completed form, the file cannot be set up and consequently the invoice cannot be processed for payment. Establishing the process in this manner takes the pressure out of accounts payable for being the bad guy refusing to make the payment.

Almost Best Practice: Few accounts payable departments have the luxury of starting over with the master vendor file. Occasionally when a new accounting system is put in, companies will take a thorough look at the master vendor file. However, it is never too late to start using best practices and it is never too late to start with a naming convention. This won't help the old data but will get the master vendor file pointed in the right direction.

Pointers for Accounts Payable: Don't fall into the trap of setting up a vendor with the minimum of information just to get the payment made. At the very minimum, insist on getting the W-9 and running it through the IRS TIN Matching program. Periodically, run a report showing all missing information from the master vendor file and attempt to fill in those blank spaces.

Worst Practice: There are so many, where to start? Here's a list of the most egregious:

Not using TIN Matching.

Allowing accounts payable and purchasing each to have its own master vendor file.

Allowing many people to set up vendors.

Allowing many people to change vendor information.

Having no naming convention.

¶203 Naming Conventions for the Master Vendor File

One of the reasons that duplicate payments occur is that there is sometimes more than one account set up in the master vendor file for the same company. Consider the case of IBM. Its account in your master vendor file could be called:

IBM
International Business Machines
I.B.M. or
I B M

Readers probably have additional variations on the few mentioned. If stringent controls are not set around the master vendor file setup and/or the files are never purged, multiple entries for the same account will ensue. Consider the following very common scenario. The first time an account is set up, it is named IBM. The next time an invoice comes in the accounts payable associate looks for International Business Machines and, not finding the entry, sets up another account on the master vendor file using the longer name. Now a third invoice arrives and is paid under the IBM name—but it is paid late so IBM must send along another invoice, marked "second notice." The accounts payable associate checks the under the longer name and finding the invoice not paid in that account, goes ahead and pays it.

Hence a duplicate payment is made. Now some reading this may think this is not a big deal; that IBM would probably return the duplicate payment, and in the case of IBM, the duplicate payment would probably eventually be returned—eventually. Researching unidentified cash is never a high priority for overworked suppliers and the funds might not come back for a month. That's one month when the firm wouldn't have use of its money. And, this is the best-case scenario.

In many cases suppliers don't return the funds—that's why duplicate payment audit firms thrive. Suppliers frequently credit the customer's account for the duplicate payment—and leave it there, never alerting the customer to the fact that the account has a credit balance.

Duplicate payments aren't the only potential problem. Multiple entries in the master vendor file open the door for unscrupulous employees to commit fraud.

Best Practice: There is one simple best practice when it comes to master vendor files. Use a standardized set of rules when naming accounts. This is sometimes referred to as naming convention. There is no right or wrong set of rules. The important thing is that there is a standard way to handle the data entry and everyone who enters data into the master vendor file, be it to set up a new vendor or update existing data, use the same standard. This convention should address every possible issue related to data including:

Whether or not to use leading articles
Whether or not to include titles
Whether or not to use spaces or initials in vendor names that are abbreviated (think IBM)
Whether or not to use punctuation in a vendor name (think Macy's)
Whether to list independent contractors and employees using the last name first or vice versa

There are a lot more issues. You need to investigate them all, taking special care not to include unusual industry-specific issues.

Almost Best Practice: There are no almost best practices here. You either use a standardized naming convention or not. A few companies have a few rules regarding naming, addressing issues like the article "The" and the use of titles and abbreviations. These are a good start in the right direction but still leave many loopholes open. For the naming convention to truly work, it has to be thorough. Otherwise, the door will still be open a crack and the unscrupulous will find ways to smash right through.

Pointer for Accounts Payable: Unless people are intimately aware of the issues relating to names like IBM and the problems they can cause, they will be incredulous when first presented with the standardized rules for naming accounts. Thus, once again, it will fall to the accounts payable manager to educate the rest of the company as to why this is such an important issue. One of the easiest ways to set standards for

addresses is to use the standards set by the US Post Office. They've thought this through, so why not take advantage of their expertise in this arena?

Worst Practices: Worst practices include:

Ignoring the issue and having no set of standardized rules.

Allowing creativity when it comes to data entry.

Not communicating the standards to all affected parties.

¶204 Updating the Master Vendor File

It would be nice if once a supplier had been set up on the master vendor file, that is it. Unfortunately, at least as far as record maintenance is concerned, is that changes occasionally have to be made to the information. People leave, companies move and phone numbers change. Additionally, if terms are included as part of the information in the master vendor file, they too change periodically.

If proper care is not taken with who can make changes to the file and who can't, the company opens itself wide open to fraud. Two simple changes to the "Remit to" address could put a legitimate payment in the hands of a crook, if a company is not careful. An unscrupulous employee with access to the master vendor file would simply change the remit to address for a supplier that is scheduled to receive a large check. After the check is cut and mailed, the employee then makes another change to the remit-to address, returning it to the correct address. By the time the supplier complains, the check will have been cashed and it becomes exceedingly difficult to trace the problem. At that point, it would probably be assumed that the check was stolen out of the mail. Who would suspect that someone had fiddled with the master vendor file? It might never even be considered.

Best Practice: Access to the master vendor file, for anything but information lookup, should be severely limited. Only a few people should be able to enter information, be it for setup or to make changes. A form should be used to standardize changes. Changes should also conform to the naming convention used when setting up the master vendor file in the first place. Those who have just read the best practices for setting up a master vendor file will note that there is a bit of overlap when it comes to making changes to the master vendor file. This makes sense. But, do not stop there. There are additional best practices that should be employed when it comes to changes to the master vendor file.

A report should be generated weekly or monthly depending on the number of changes made on average to the master vendor file. The report should detail all the changes made to the file in the given time period. It should include the names of the person requesting the change and the person authorizing the change. It might also include the date the last change was made. This report should be given directly to a senior-level executive and should be reviewed line by line for any odd looking entries. The fact that this report is generated and reviewed should be common knowledge.

In all cases, companies should have the ability to generate this report whenever needed.

Almost Best Practice: While it is desirable that a senior-level employee (such as an AP manager) review changes made to the master vendor file, few will be willing to do this. They simply do not have the time. They can, however, delegate it to someone on staff.

Pointer for Accounts Payable: In the likely event that the senior executive doesn't review the report, ask that it be given to someone who will.

Worst Practices: Worst practices include:

Having no formal process for inputting changes to the master vendor file.

Having no review process of the changes made to entries in the master vendor file.

Having no limits on who can make changes to the file.

¶205 Master Vendor File Cleanup

At many companies, once a vendor gets into its master vendor file, it stays there forever. In a perfect world this would not be a problem. However, if an account is not used for a while and then the vendor becomes active, often a new master vendor file is set up. Then, and especially if no strict naming convention is used, there will be two or more master vendor file entries for the same vendor. This can lead to duplicate payments

or worse. When a duplicate invoice arrives, and one of the master vendor files checked and no payment is found, a duplicate payment will be made against the second vendor file. Even worse, if an employee bent on fraud becomes aware of an inactive vendor file, the employee can use the inactive file as a cover for fraudulent practices.

Best Practice: Once an account has been inactive for over a year, it should be cleansed from the company's master vendor files—or moved to inactive status. The activity should be maintained for several years. The policy and procedures for master vendor file cleanup should be incorporated into the accounts payable and purchasing formal written policy and procedures guidelines. It is critical that the old data be maintained. In ideal circumstances, the cleansing of the master vendor file is an ongoing task, sometimes performed quarterly.

Maintaining the master vendor file should be an ongoing process and not a one-shot project. The experts like to say that master vendor file maintenance should be a process, not a project.

There are certain events that trigger a cleansing of the master vendor file when it hasn't been done in the past. They include, but are not limited to:

The installation of a new accounting package
A merger
An acquisition
The hiring of a new controller or CFO

Take advantage of these events to bring up the issue of master vendor file maintenance and introduce best practices in this area.

Almost Best Practice: If the issue is not going to be addressed on an ongoing basis, the once-a-year review is probably an acceptable alternative.

Pointer for Accounts Payable: If the master vendor file has never been purged and a new accounting system is being put in place, many companies choose to start over from scratch rather than try and purge the existing file. While this is a lot of work, it is sometimes easier than trying to sort through the mess that currently exists. It is not unusual to hear reports from companies that go through their master vendor file for the first time that indicate the company only kept 30 percent of the vendors from its old master vendor file.

Sometimes folks will ask what I think of hiring a temp to clean up their master vendor file for them. Because, let's be honest, cleaning up the master vendor file is not a fun job. While a temp probably could run some reports, at the end of the day, the final review is going to have to be done by someone who knows the business rather well. This means either the accounts payable manager or a seasoned supervisor.

Worst Practices: Worst practices include:

Never cleansing the master vendor file.
Haphazardly cleansing the master vendor file.
Having no one with direct authority or responsibility for the maintenance of the master vendor file.

¶206 Self-Service Master Vendor Files

Automation has finally found its way into the accounts payable function, and the master vendor file is no exception. A small but growing number of companies have developed online portals that allow their vendor to input their own information. There's a lot to be said about this approach. First, it gets the vendor to do some of the work, and for most organizations that's a plus. But, on the more serious side, it makes the vendor responsible for its own data, including updates. This has become increasingly important given some of the new electronic payment frauds and scams.

Additionally, it makes it easy for the company owning the portal to ping by e-mail its vendors once a year asking them to update contact information. This is a task that rarely gets done with traditional master vendor files. Many who use this type of repository for vendor information find that it creates benefits far beyond those of a traditional master vendor file.

These online vendor portals are quite expensive to build. However, there are alternatives. There are third-party models available for sale and these can be used quite effectively. Some of them will even do TIN Matching and other data verification for you.

Best Practice: Send new vendors a link that provides them access to the vendor portal so they can set up their information in your master vendor portal. These portals are online, utilizing a secure connection. Once the information is uploaded, someone on staff needs to review it to ensure it conforms to your coding/naming standards. There's no way you are going to get the vendor to enter data according to your standards. If the vendor only adds some of its information but not all, the portal can automatically send reminders asking for the missing information.

As mentioned above, at least once a year an e-mail should be sent to all active vendors asking them to update their contact information. Without this important task, the contact information gets stale and within a few years is almost useless.

Most importantly, for those making ACH payments, the vendor is responsible for inputting its bank account information. If it changes bank accounts, it can go in at any point and update its bank account information. That should be the only way that information gets changed. If someone from the vendor contacts your organization asking you to change the data, direct them to the portal. If it is a legitimate call or e-mail, they will make the change appropriately. If it wasn't, you'll have just thwarted a potential fraud.

Almost Best Practice: This is a new area, so appropriate practices are still emerging. Use of an online self-service vendor portal is considered a best practice in and of itself. Since organizations utilizing these portals typically are best practice organizations, to date, we haven't seen the emergence of almost or worst best practices.

Pointer for Accounts Payable: Whether you purchase this from a third-party or take the more expensive route of building in-house, these portals are not free or cheap. Hence this probably means a budget item. It means making a presentation to management, demonstrating the benefits, and asking for a budget allocation. If you are extremely lucky, you'll present the concept and your company will see the light and give you the okay to go ahead with either the purchase or development.

However, that is not the likely outcome the first time you bring up the topic. This is something that will have to be talked about for some time. So, get started now. If you are making ACH payments, emphasize the reduction in the fraud risk potential. That can be a huge selling point. As time goes on, we expect this self-service portal approach to vendor information will become more commonplace.

Worst Practice: So far—none. Let's hope it stays that way!

Review Questions

6. Who should have the ability to add new vendors to the master vendor file?
   a. Anyone in the accounting department
   b. Anyone in purchasing
   c. Only the few people whose job it is to handle master vendor file data
   d. Anyone in accounts payable

7. When should a new vendor be set up in the master vendor file?
   a. Whenever the vendor data has been collected
   b. Before the first purchase order is written
   c. It doesn't matter
   d. Before 1099s have to be issued in January

8. Which of the following is not a worst practice when it comes to developing a naming convention?
   a. Ignoring the issue and having no standards
   b. Allowing creativity when it comes to data entry
   c. Using a rigid naming convention
   d. Not communicating the standard to all affected parties

9. Updates to information in the master vendor file should be reviewed using which of the following approaches?
   a. Updates don't need to be reviewed.
   b. A regular report showing changes given to senior management for review.
   c. Updates should be reviewed by the person who requested them.
   d. A clerk in accounts payable can review the updates.

¶300 Invoice Processing

Learning Objectives

Upon completion of this chapter, you will be able to:

Create effective invoice receipt practices

Establish effective data entry rules for invoice processors

Construct best practice invoice handling routines

Invoice processing is the core of the accounts payable function. Without it, the tasks typically handled in accounts payable could probably be assigned to other units in accounting and purchasing. In this chapter, we discuss:

Receipt of Invoices
Invoice Handling: Approvals
Invoice Data Requirements
Verifying Invoice Data
Invoice-Coding Standards
Handling E-Mailed Invoices

¶301 Receipt of Invoices

Receiving invoices in a timely manner is critical to an efficient accounts payable function. Yet, this issue is frequently ignored because it's one of those small matters that those not intimately involved in accounts payable don't realize can have a huge impact. Invoices that are delayed in getting to accounts payable often result in the vendor sending a second invoice. In a best-case scenario, that means extra work for accounts payable in identifying that second invoice and *not* paying it. Unfortunately, a few of those second invoices do get paid, and that money is rarely returned without some sort of investigation on the part of the accounts payable staff or its agent. In either case, more work for accounts payable translates into a higher expense for the organization.

Best Practice: Invoices should be received in one centralized location. Traditionally, this has meant a post office box, with the mail being delivered to accounts payable for processing. However, some vendors are refusing to mail invoices, citing the expense and work associated with that task. They insist on either e-mailing or faxing. Thus, we now have to expand the definition of one centralized location to include an e-mail delivery point and a fax delivery point.

The e-mail address should be a generic address (something like ap@abcompany.com) that can be accessed by several people. The fax number should be for a fax machine that will be used for nothing but the receipt of invoices. Ideally, it should be in a secluded corner in the accounts payable department, as far away from others as possible. This will keep them from being tempted to use the fax, and then inadvertently picking up an invoice or two when retrieving their document.

In some organizations, the purchasing department prefers to receive the invoices first. This can create additional work for accounts payable, especially if some of the approvers are tardy in their review of invoices submitted for payment. The ideal solution to this issue is electronic invoicing, be it a home-grown system, a third-party offering, or even invoices e-mailed to the company. With an electronic document, everyone can have access to the invoice almost simultaneously and there is an electronic audit trail showing who got what when—and when an approved invoice was sent to accounts payable for payment.

Almost Best Practice: There are some organizations, albeit a dwindling number, who still refuse to take invoices by e-mail or fax. For those organizations, one centralized address for the receipt of invoices is suggested. However, they are advised to rethink their position on requiring paper invoices. Paper is disappearing fast, and some vendors are starting to charge for sending paper invoices.

Special Pointers for Accounts Payable: By giving several people with access to the e-mail account used to receive invoices, you take the onus off one person. Additionally, there are fewer concerns if the person responsible for retrieving those invoices is unexpectedly absent. Finally, you can get the best of both worlds by combining your fax number with an e-fax facility, turning those paper faxes into electronic documents before you ever receive them. This is not an expensive option and is within the financial reach of virtually every organization.

Worst Practice: Having no policy regarding the centralization of the receipt of invoices. While it is not desirable to have purchasing receive invoices first, it is better than having no policy and allowing invoices to be sent wherever the vendor chooses.

¶302 Invoice Handling: Approvals

In an ideal world, if all purchase orders are filled out completely and correctly, if receiving thoroughly checks all packing slips, and vendors create accurate invoices, the accounts payable department should be able to pay the invoice without input from any other party. However, few companies are at this point. Even at those companies where the documentation is good, management often demands that the original purchaser approve the invoice for payment.

Best Practice: At most companies, only certain people can approve invoices for payment. Most companies limit this ability by rank, job responsibility, type of purchase, and sometimes even the dollar amount. In the best of circumstances, the company's leaders should have given these approvers authority and accounts payable should have copies of these board authorizations.

Copies of the list, if it exists in paper format, should be given only to those who need it, and in all cases should be filed away carefully. The list should not be hung on the wall for easy reference or left lying on a desk where anyone walking by could see it and easily make a copy. When the list is updated, as it periodically will be, old copies of the list should be destroyed.

Just because an invoice arrives in accounts payable with a senior executive's signature on it does not mean that the senior executive actually approved the invoice. To protect the accounts payable staff, the department should have signature cards in accounts payable containing the actual signature of anyone authorized to approve invoices. And, it should be the executive's real signature, the one he or she uses every day.

More than one executive has taken the time to sign a signature card carefully, when in actuality everything else has an illegible scrawl on it. In these cases, the signature card should have the illegible scrawl as well, or the accounts payable associate might suspect fraud when the signature cards are checked.

We are not suggesting that these cards be checked for every invoice that shows up. However, spot-checking once in a while is not a bad idea. And, obviously, if a suspicious-looking signature arrives on an invoice, the signature cards should be checked immediately.

Ideally, invoices will arrive electronically. When an invoice is received electronically, it should be forwarded to accounts payable for processing. Using workflow, the accounts payable department can forward the invoice for approval to the appropriate approver. This is based on information provided on the invoice integrated with the approver list discussed above.

Companies should include in their workflow programming an escalating approval feature. What this means is that if the first approver does not respond within a given timeframe, say five days, the invoice is automatically routed to the next higher approver in that chain of command. This takes care of not only tardy approvers, but also vacations and unexpected absences. It simultaneously creates an audit trail for everyone to see. No longer can purchasing claim it sent an invoice back to accounts payable when it is still in the department. Finally, the audit trail feature combined with escalating approvals make it far less likely that managers will relegate invoice approval to the bottom of their work—especially when not approving invoices may actually create more work for their immediate supervisors.

Having all invoices come first to accounts payable also introduces another control against employee fraud. Invoices cannot be altered, nor can they show up out of the blue with what looks like an executive's signature on them. By scanning the invoices and forwarding them for approval, it makes it all the harder for a scheming employee to forge a boss's signature.

Almost Best Practice: In the absence of executive authorizations, accounts payable should have a list of who can approve what purchases. A high-level executive at the company should sign off on this list.
Special Pointers for Accounts Payable: Be careful of admins who approve for their bosses. While this might make life easier for the boss, it is a complete breakdown of appropriate internal controls and should not be tolerated.
Worst Practices: Worst practices include:

Not having a list of authorized approvers.
Allowing anyone to submit invoices for payment.

¶303 Invoice Data Requirements

You would think that vendors would instinctively include all information on an invoice needed to get it paid quickly and accurately. But, this is an issue many don't take seriously. They send an invoice in for payment with no data indicating who ordered the item. This makes it extremely difficult for accounts payable to get the invoice approved and scheduled for payments. What's more, some of these vague invoices are actually fraud.
Best Practice: Invoices that arrive without the name of the purchaser or a PO number should be returned to the vendor with a polite note stating your organization's requirement that this information be included on all invoices. Otherwise, someone in your organization is going to waste a lot of time trying to figure out who should get the invoice for approval purposes.
Almost Best Practice: To be honest, sometimes it is pretty easy to guess who placed a particular order. If you can tell without too much trouble, it is probably okay to process the invoice without going back to the vendor. However, if you do so, the vendor will never get it right and will continue to send invoices without proper documentation.
Special Pointers for Accounts Payable: While sending invoices lacking the purchaser's name back to suppliers may lead to a smoother accounts payable operation, not all management teams are going to think this is a great idea. Thus, it might be a good idea to get management on board before instituting this policy.
Worst Practice: Having no policy on this issue.

¶304 Verifying Invoice Data

In an ideal world, a company would sell its customers products and would in due course be paid for those goods according to the pre-negotiated payment terms, once the purchaser had verified it had received what it had ordered. (Some reading this may recognize this as the underlying principle of Evaluated Receipt Settlement, or ERS.) Unfortunately, there is a lot that can and often does go wrong with this simple scenario. Some of the things that go awry include:

Terms on the invoice not matching what was negotiated
Partial shipments
Damaged goods
Prices on the invoice not matching the negotiated prices
Inclusion or exclusion of related charges such as freight, insurance etc.
Sales and use tax charged/not charged

Consequently, the process for paying for goods can be quite complicated—especially when it comes to verifying the suppliers' invoices.
Best Practice: Once an invoice has been approved (if that is required), a three-way match should be performed on all invoices over some minimal level. Small-dollar invoices will be addressed further on. The accounts payable associate should match the PO against the invoice and packing slip to verify that the goods ordered have been received and the price and other fees (tax, insurance, freight, etc.) are as agreed.

Differences must be resolved before the invoice can be paid. If the difference is in the pricing, the better price should be taken. If the lower price happens to be on the invoice, not only should the lower price be taken, but purchasing should be also notified. The reasoning for this is that if a lower price is put on an

invoice, it probably indicates that the supplier is offering a lower price to other customers and purchasing should pursue that for your company.

Discrepant invoices should be resolved quickly. Ideally, the manager should track all discrepant invoices to make sure that they don't drag on unresolved for months on end.

The process described above can be done online. The best systems now have online dispute resolution features built in—especially when using electronic invoicing.

As alluded to above, some companies use a process known as evaluated receipt management (ERS). This eliminates the invoice from the process—the document that many accounts payable professionals believe causes the most problems with the three-way match. Using ERS, the accounts payable staff receives POs from purchasing, and when it gets the packing slip from receiving, it pays according to the terms indicated on the PO. Companies that insist that the PO be completely and accurately filled out have taken the first step towards being able to get rid of the invoice. If the PO line is under control and the professionals on the receiving dock thoroughly check the packing slips on incoming orders, a company could effectively use ERS. Use of ERS has to be negotiated with suppliers before implementing. This is also known as pay-on-receipt.

In addition to verifying that the PO matches the invoice regarding price and other fees, many companies are now taking the verification process one step further with a contract management function. As the title implies, invoices, sometimes after the fact, are checked against contracts to ensure that pricing, terms, and so on, are charged as agreed upon in the master contract agreement. This typically only occurs with major suppliers.

Almost Best Practice: Obviously, going through a thorough three-way match can be an expensive process for small dollar invoices. There is an alternative. First the company must set a dollar cut-off for use of one of the alternatives. This cut-off can be as low as $100 or as high as $5,000 or $25,000. Companies that institute one of the following can start small and then increase the level as they get comfortable with the process. Corporate culture will also have an impact.

The first approach is referred to as *negative assurance* or *assumed receipt*. When accounts payable gets an invoice for an amount under the agreed-on level, an e-mail is sent to the person who would approve the invoice indicating key factors, such as payee, dollar amount, and so forth. If imaging is being used, a copy of the invoice can be attached to the e-mail message. If accounts payable does not hear from the approver within a preset number of days, typically five to ten days, the invoice is paid. The goods are assumed to have been received unless the purchaser notifies accounts payable to the contrary.

Special Pointers for Accounts Payable: Many approvers don't check the information on invoices. Nor do they bother to verify that the invoice they are approving today wasn't approved last week or last month. That's part of the reason so many duplicate payments occur. It's also why the three-way match and ensuring that associated purchase orders and receiving documents are extinguished.

Worst Practice: Simply relying on the approval signature to pay the invoice without verifying the veracity of the information on the invoice.

¶305 Invoice-Coding Standards

Coding invoices is one of those functions that no one really focuses on too much. However, handled ineffectually, it can and does lead to duplicate payments and opens the door to fraud. It is one of those functions that at first glance seems like a non-issue. What do you mean you want standards for coding invoices? The words "control freak" may be running through your mind. But consider the following simple case. Consider the company AT&T. Its name could be coded:

American Telegraph and Telephone
AT&T
A T & T
A T and T

Even if you eliminate the first entry as unlikely, it is easy to see how two competent accounts payable specialists could code the company name in any one of several ways—none of which would be inaccurate. Each data element has similar issues.

Best Practice: Develop a rigid coding standard that addresses every possible issue related to invoice data entry. It should be consistent with your naming convention used for the master vendor file. It should be used by all processors and *no* creativity permitted when it comes to data entry.

There is no right or wrong way data should be entered, just as long as everyone does it the same. At a minimum, your coding standard should address:

How you handle abbreviations

How you handle spaces, periods, and other punctuation in a name

Whether you enter an individual's name with first name first or last

When it comes to setting a standard for entering addresses, the easiest way to set this is to rely on the standards set by the US Post Office.

When it comes to entering invoice numbers, special care should be taken, especially if you have only a limited number of fields to enter the invoice number. Do you code leading zeros or not? There is no right or wrong answer to whether or not to code leading zeros. Each company must decide if it wants to code them, and then set a policy. Each aspect of invoice coding policy should be addressed, a policy set and then communicated to all processors. It may seem excessive, but it will eliminate numerous problems down the road.

If you have the space limitation, you will also want to consider whether to eliminate extra digits at the beginning of the invoice number or the end, if you do not have enough space. Most would eliminate leading digits rather than those at the end.

Some with unlimited space rely on the old "key what you see." Don't forget to address any industry peculiar issues you may have.

Almost Best Practices: Almost best practices include:

If no invoicing coding standard exists, use the standard naming convention used when setting up master vendor files. While not perfect—it doesn't address certain issues peculiar to invoices—it is better than nothing.

If an invoice-coding standard does not exist, at a minimum, establish policies for coding the invoice number. If various staffers code invoice numbers differently, duplicates will seep into the process.

Special Pointers for Accounts Payable: Even with a clear policy, processors will occasionally veer off. As soon as this is noticed, the accounts payable manager needs to correct the situation, as without conformity on this issue, duplicate payments will slip through. If the thought process behind the policy is explained, most processors will understand and abide by it.

Worst Practice: Not having a policy at all. Each processor will use his or her best judgment, leading to numerous duplicate payments.

¶306 Handling E-Mailed Invoices

Given that virtually every company is now receiving invoices delivered by e-mail, it is time to look at best practices around that process. What's more, because of the low cost associated with e-mail, many of the invoices are being sent multiple times—and occasionally are mailed as well.

Best Practices: Your approach to handling e-mailed invoices should include the following steps:

Set up a separate e-mail address for the use of receiving invoices.

Access to this separate e-mail address should be given to several people, so invoices do not go unprocessed in cases of unexpected absences.

Suppliers should be discouraged from sending invoices to any e-mail address other than the special one set up for invoices.

All suppliers, as well as all employees who may receive invoices, should be notified of this separate e-mail address and instructed to send invoices to it, and no place else.

Set up a protocol for the saving of invoices, if you are not using an e-invoicing module. This will ensure that when the same invoice is received more than once, it doesn't get saved as two separate invoices.

If you are using an e-invoicing module, set up procedures to have the e-mailed invoices uploaded. This may even be automated.

Create standardized procedures for the handling of invoices received by e-mail, ideally one that does not involve printing the invoices. It should match the process used with invoices received in the mail. This will help weed out invoices sent using both mediums.

Vendors who send invoices more than once or to multiple parties should be contacted and given instructions on the proper submission of invoices. Do not expect them all to comply. Many are primarily interested in getting paid not in making their customers' accounts payable department more cost effective.

Worst Practice: Allowing vendors to send invoices wherever they please.

Special Pointers for Accounts Payable: The volume of invoices being sent via e-mail is exploding. In some cases, organizations are receiving more than 50 percent of their invoices by e-mail. Therefore, it is critical that every organization have a policy to address this—for it is only a matter of time before paper invoices become a thing of the past.

Review Questions

10. Which of the following describes the recommended best practice for the receipt of invoices?
    a. Invoices should go wherever the supplier chooses to send them.
    b. Invoice receipt should be centralized with one postal address, one e-mail address, and one fax number.
    c. Invoices should only be received by postal mail.
    d. Invoices should only be received by e-mail.

11. The ability to approve invoices should be guided by which of the following?
    a. Delegations of authority from the board of directors
    b. Practices that evolved
    c. What was always done in the past
    d. Directives from the AP manager

12. Invoices should be returned to the supplier if they do not contain which of the following pieces of information?
    a. The headquarters address
    b. The website address
    c. A PO number or name of the purchaser
    d. A tax ID number

13. The three-way match involves matching all of the following documents except which one?
    a. Receiving document
    b. W-9
    c. Purchase order
    d. Invoice

¶400 Invoice Problems

Learning Objectives

Upon completion of this chapter, you will be able to:

Define effective practices when short-paying invoices

Develop standards for handling unidentified invoices

Establish a process for managing discrepant invoices

Unfortunately, invoices rarely arrive in perfect condition. For most organizations, there are typically problems with the data on the invoices or data missing from the invoice. That's part of the reason we can't take a "you get an invoice, you pay an invoice" approach to accounts payable. For if we took that approach, we'd pay more than we should and some invoices would get paid two and three times. In this chapter, we discuss:

Short-Paying Invoices
Handling Unidentified Invoices
Handling Invoices Without Invoice Numbers
Discrepant Invoices
Second Invoices with a Different Invoice Number

¶401 Short-Paying Invoices

When most companies print their checks, they print identifying information on the accompanying remittance advice. The most important piece of information usually is the invoice number. It gives the vendor the information it needs to apply the cash to the correct account. Certain companies send along a stub with their bills. They require that this stub be returned with the payment. This is so the vendor can apply the cash payment correctly.

However, as those reading this are well aware, the amount of information that can be included on a remittance advice is severely limited. When an invoice is short paid, and the reasons for the short payment are not communicated to the vendor, it is inevitable that the vendor will call accounts payable for an explanation. Unfortunately, by the time the vendor gets around to calling, days, if not weeks, will have passed and the accounts payable associate will have long forgotten why the deduction was taken—assuming that the person getting the call was the person responsible for the deduction in the first place.

Deductions are frequently made, for various reasons including:
Discounts for early payment
Short shipments
Damaged goods
Advertising allowances
Prior credits
Insurance or freight incorrectly charged
Pricing adjustments
Over-shipments
Advertising allowances

Best Practice: Whenever invoices are not paid in full, it is important—not only to keep the accounts payable department running smoothly, but also to help maintain good vendor relationships—that the reasons for the deductions be communicated in as much detail as possible to the vendor. This does not ensure that the vendor will agree or won't call, but it will eliminate many needless calls.

Thus, even though it might take a little extra time when the invoices are being processed, put detailed notes in the file as to the reason for the deductions. This can be important if the matter is raised after several months or in the case of an audit. The detailed notes will be worth their weight in gold.

The best approach is to include a detailed breakdown for the reasons for the deductions. Those making electronic payments will find that this information can often be shared as part of the electronic remittance advice. Alternatively, it can be e-mailed to the person at the vendor doing the cash applications. This is extremely important because some vendors refuse to accept electronic payments because of the cash application problems. If you can demonstrate that you've solved this problem, they will be more likely to accept electronic payments from your organization.

Almost Best Practice: A low-tech approach, especially useful with payments made by check, is to develop a form listing the most common reasons for short payments. Then the accounts payable associate can simply check off the appropriate field and attach it to the check. These forms should be developed based on the company's past history and industry. They should be periodically reviewed to ensure that they contain all relevant factors. There should be several blank lines at the bottom for any details that will be useful to those using the form.

There is a small group of accounts payable organizations that never short-pay an invoice. They hold the view that they will not pay an invoice until it is prepared correctly. They return these invoices demanding that the supplier correct them, and when the invoice is prepared satisfactorily, they pay it.

Special Pointer for Accounts Payable: Don't expect that the form will put an end to vendors' complaints. It will simply eliminate one round of calls and one round of investigations as the information typically provided in that round will have been provided on the form.

Worst Practice: Sending along a short payment with no explanation. The vendor will call, and even worse, may end up putting the company on credit hold thinking it is owed money. The name of the game in this case is communication—you can't have too much of it.

¶402 Handling Unidentified Invoices

More often than you'd think, an invoice shows up in the accounts payable department with no identification as to who ordered the product. Occasionally these invoices will float from desk to desk throughout the company before finding their way into accounts payable. Sometimes by looking at what is included on the invoice, a savvy accounts payable associate will be able to figure out who the likely purchaser is and will then forward the invoice to that person for approval.

However, that is frequently not the case, especially in the case of generic goods like printer cartridges or paper for the copy machine. Often the dollar amount involved is small and does not appear to be worth the time and effort to research who ordered the goods. These are especially problematic as there is a higher incidence of fraud with these invoices than might be expected.

Best Practice: The best approach is to send these unidentified invoices back to the sender, asking it to indicate who ordered the goods. To be clear, an unidentified invoice is one that does not have either a purchase order number or name of a requisitioner. Include a polite letter stating that it is your organization's policy to require this information so you may get the invoice paid as quickly as possible. By showing the vendor how it will benefit by including this information, it will be more likely to adapt to your requirements. By the way, this requirement, as well as any other accounts payable requirements, should be included in your terms and conditions provided to the vendor at the beginning of the relationship. This stance is especially important in the case of small-dollar items. (See Worst Practice below).

How effective is this approach? A manager shared that a company she worked for had insisted on sending such a letter to a vendor that was a foreign company, and she thought it just didn't realize how the US worked. So, she fought hard against it—and lost. The letter was sent. Within three months after the first letter was sent, the company had 100 percent compliance with this requirement. The manager described the outcome as "ridiculously easy to accomplish." No one was offended, or if they were, they didn't complain. For at the end of the day, vendors want to get paid as quickly as possible with as little fuss as possible.

Almost Best Practice: If it is not feasible to simply return the invoice, pick up the phone and call the vendor. When provided with the information, request that in the future the vendor include the requestors' names on invoices. If this is a recurring problem, keep a list of vendors who routinely omit the purchasers' name, along with the employees' names who regularly order from these companies. Again, ask the employees to request that their name or department be included on all invoices.

Special Pointers for Accounts Payable: This is one of those headaches that in all likelihood will never go away completely. However, accounts payable can and should do what it can to minimize the problem. By working with these suppliers, many of whom are small and will be amenable to listening to suggestions (rather than demands), accounts payable will be able to make a dent in the problem.
Worst Practice: Simply paying for the goods, reasoning that the dollar amount is too small to bother with. This can quickly get your company on the sucker list. More than a few companies prey upon overworked accounts payable departments. They send along invoices for goods not ordered, knowing full well that small-dollar invoices are often paid without authorization. Once you pay that unidentified invoice once, your company will be hit over and over again—and probably for increasingly larger amounts of money as time goes on.

¶403 Handling Invoices without Invoice Numbers

Invoice numbers are extremely important when it comes to processing invoices. They are the primary way that most companies identify invoices and check to see if they have already paid a particular item. An invoice without an invoice number is much more likely to be paid twice than one that has this key identifier. Yet a surprisingly large number of invoices routinely arrive without invoice numbers, creating all sorts of headaches for the companies that receive them.

That's just the beginning of the problems. When an accounts payable associate goes through its computer files, he or she will search to see if the particular invoice number has been paid. Additionally, most accounting programs require an invoice number in order to generate a payment.

So, to get around these problems, most companies assign invoice numbers to those invoices that arrive without these important identifiers. If not done in a manner that will create unique identifiers, the system will regularly dump out a large number of payments when any duplicate payment check programs are run. The key is to do it in the manner that does not create more problems than it solves.
Best Practice: This is another area where best practice thinking has changed. Today, just about everyone, even the smallest businesses, has access to computers. So, a unique invoice number should be part of your requirements. Take any invoices that arrive without an invoice number and return them to the vendor with a polite note explaining your requirement that every invoice have an invoice number.
Almost Best Practice: The important facet of this discussion is to recognize that invoices without invoice numbers are a problem and to devise a system to deal with the issue that does not create additional problems at the same time. The best technique is probably to make up a dummy number that includes some unique identifier to the vendor, for example, a combination of digits from the vendor's phone number and a running total.
Special Pointers for Accounts Payable: Invoices without invoice numbers create huge headaches in accounts payable. Even if you have a wonderful system for creating an invoice number, that number will not be of any use when discussing open items with the vendor as it does not know the invoice number and if you refer to that identifier, the vendor will have no idea what you are talking about.
Worst Practices: Worst practices include:

Using the date to assign an invoice number is likely to cause problems, as you will probably end up with duplicate invoice numbers. Some use a combination of the vendor number and the date. Again, this can cause trouble if you receive more than one invoice from the same vendor on the same day.

Creating an invoice number using the account number when it bears any relation to the tax identification number or a person's social security number. There have been instances where unscrupulous employees (yes, there are a few of those) have taken the social security numbers and used them in an unscrupulous manner.

¶404 Discrepant Invoices

Discrepant invoices are those that don't match what is on the receiving document and/or purchase order. Many organizations try and resolve these problems before paying the invoice, refusing to make partial payments. This works well in theory, but in practice there can be some problems.

The most obvious is that the invoice problem is not resolved before the due date, thereby making it impossible to pay the invoice on time. Delays in communication and finding the necessary information to resolve the discrepancy are common. Unfortunately, when the invoice is not paid, the vendor often issues a second invoice looking for its money.

This is not an unreasonable approach on its part. When that second invoice arrives, accounts payable has to identify it as a second invoice. That takes unnecessary time and effort. What's more, some of those second invoices slip through and get paid. This is not a good thing as few duplicate payments are repaid without some additional work on the part of the customer.

Best Practice: Have a policy requiring all discrepancies be resolved before the due date. While it is fine to have this as a policy, in reality you will still have discrepant invoices on the due date. You need to take steps to keep on top of those issues. The best way to do this is to have the manager track discrepant invoices and follow up with the processor responsible for reconciling the discrepancies on a very regular basis.

Some accounts payable departments regularly produce a report showing the number of discrepant invoices by processor. Some of these reports also age the discrepant invoices. This is one list that no one wants their name on the top of!

Once you have your report of discrepant invoices, probably in Excel format, you might want to add a few columns. You can use these columns to identify the name of the processor, the name of the vendor, the associated purchasing professional, and the reason for the discrepancy. If you record all this information on a regular basis, you can use it to do some analysis once you've collected several months of data.

When you've accumulated enough data, go back and study it to see if you can identify common problems or root causes. For example, if you have an inordinately high number of errors associated with one processor, he or she might need some additional training. If the problem seems to be with a particular vendor, a discussion with that vendor to determine what the problem is might be in order.

Your analysis should not be a one-shot deal. You should look at the data every few months. For just as you fix one problem, another is likely to rear its ugly head.

Almost Best Practice: This is an area where there are no almost best practices. Tracking is a must, if you want to keep the discrepant invoice issue under control.

Special Pointers for Accounts Payable: It is imperative that processors keep on top of their discrepant invoices. For without regular follow-up, the invoices are apt to languish and those inevitable second invoices will begin to appear. What's more, unresolved discrepant invoices have a way of turning into rush payment requests, or even worse, the vendor will use your open credits to clear away the outstanding invoice. While the vendor may think it is doing you a favor, in actuality it is using your credits to pay for something your organization had no intention of paying for.

Worst Practice: Not tracking discrepant invoices at all. Without tracking, discrepant invoices end up at the bottom of the pile and contribute to the idea that accounts payable is the black hole where invoices go never to be seen or heard from again.

¶405 Second Invoices with a Different Invoice Number

Second invoices with a different invoice present a unique challenge for the organization trying to avoid making duplicate payments. For starters, this is just one more issue that highlights the fact that you cannot rely 100 percent on the invoice number to identify a potential duplicate. Therefore, duplicate payment identification routines must rely on more than the invoice number. Here are some tactics that will help.

Best Practice #1: Following best practices for invoice processing is probably the single best tactic you can use to combat this nasty problem. These include using rigid coding standards, the three-way match, and immediate extinguishing of the purchase order and receiving document when the payment is scheduled.

Best Practice #2: As soon as you identify vendors who use a different invoice number, add them to the small list of vendors whose invoices are double-checked.

Almost Best Practice: You can try talking to the vendor and asking it to use the original invoice number, but don't expect this to be overly successful. At the end of the day, the vendor will have established practices, and it is not likely you will be able to change them.

Special Pointers for Accounts Payable: Some believe that vendors who use this approach do so purposely to try and get some of their customers to pay twice. You will never be able to prove or disprove this theory. So, your best defense is to follow best practices and make sure you are not one of their customers who double pay.

Review Questions

14. Which of the following is ***not*** a legitimate reason for short-paying an invoice?
    a. Taking an early payment discount
    b. Taking a deduction for problems on another invoice
    c. Taking an advertising allowance
    d. Using an open credit from an earlier transaction

15. Paying small-dollar invoices without knowing who ordered the items included on the invoice is a poor practice for all of the following reasons, ***except***:
    a. The invoice could be fraudulent and no one placed the order.
    b. It is efficient.
    c. If you pay a fraudulent invoice, you are likely to get more.
    d. Your financial statements will be negatively affected if you pay for something never ordered.

16. Which of the following is not a worst practice when it comes to creating invoice numbers?
    a. Using the date as an invoice number
    b. Using a social security number as part of the invoice number
    c. Processing the invoice without an invoice number
    d. Insist that all invoices have invoice numbers

17. When analyzing discrepant invoice data to see if you can identify root causes, you should categorize invoices by all of the following, ***except***:
    a. Invoice number
    b. Purchaser
    c. Vendor
    d. Processor

¶500 Checks

Learning Objectives:

Upon completion of this chapter, you will be able to:

Create effective processes for printing and signing checks

Design a suitable process for storing check stock

Despite the fact that checks are an expensive, inefficient way to make payments, virtually every organization in the United States relies on them heavily to facilitate payments. In most of the rest of the world, payments are largely made electronically. So, we're going on record as noting that electronic payments are a more proficient way to fulfill financial obligations. However, due to their heavy use in the United States, we feel it important that we address the issues surrounding them. In this chapter, we discuss best practices related to:

Approach to Paying by Check
Check Printing
Check Signing
Check Stock Storage
Distribution of Checks
Check Fraud
Use of Payee Name Positive Pay

¶501 Approach to Paying by Check

As mentioned above, paying by check is a rather inefficient way to pay invoices and other obligations. With the emergence of the Automated Clearing House (ACH) network in the United States, there is now a low-cost alternative to the paper check nightmare. Not only is it a less expensive approach, it also eliminates certain inefficiencies from accounts payable and solves certain problems.

For example, with no uncashed checks there is no need to do due diligence on uncashed checks and then remit the funds to the states as unclaimed property.

Best Practice: Actively encourage all vendors to accept payments electronically or accept purchase card (p-card) payments. Both methods reduce the number of paper checks issued. Develop a plan to systematically approach vendors asking them to accept electronic payments. Do whatever you can to reduce the number of paper checks issued.

Almost Best Practice: If you aren't ready to go full steam ahead with plans to pay vendors electronically, at least pay those vendors electronically who request such payments. And begin to make plans to expand your electronic payment horizons in the near future.

Special Pointers for Accounts Payable: The accounts payable arena is changing, and payment methodology is leading the charge. As the number of individuals paying their own personal bills electronically continues to skyrocket, executive reluctance to electronic payments should subside.

Worst Practice: Refusing to pay any vendor in any manner other than with a paper check.

¶502 Check Printing

Companies print checks as frequently as every day and as infrequently as once or twice a month, depending on numerous factors, which can include:

Corporate culture
Whether they are trying to encourage vendors to accept electronic payments
Cash management practices
Number of checks printed
Check-signing practices

Check-printing practices
Efficiencies in invoice handling procedures

As bizarre as it may seem, a few companies print checks only once or twice a month, not because that is an efficient way for them to run their business, but because they feel it gives them greater control over their cash flow. They can tell a vendor that they will print their check at the first opportunity—which will be in two or three weeks in the very next check run. Unfortunately for them, this excuse often ends up with the vendor threatening to put the company on credit hold, which in turn results in manual rush (and very inefficient) checks. As those familiar with the implications of rush checks are well aware, this can in turn lead to an increase in duplicate payments and potential fraud.

Obviously, the size of the company and the number of checks it needs to issue will directly affect the frequency of its check runs.

Best Practices: While we might argue that the best practice when it comes to printing checks would be to not print any checks at all—to convert to a 100 percent electronic medium relying on ACH, this is not a realistic approach at the current time. Given that checks are here at least for the short run, let's take a look at the state of check printing today.

Regardless of the type of printing used (mainframe or laser), AP departments should make sure all affected parties know not only what their check run schedule is but also the cutoff points. If an approved invoice or check request needs to be received in AP by noon on Thursday in order to be included in a Friday check run, this vital information should be shared. Otherwise, people will show up in AP on Friday morning with requests, expecting them to be included in that day's check run. In the long run, it is far better to spend the time communicating this information (verbally, in writing, and on the department's intranet site) with everyone who could possibly be affected.

The process for printing checks in corporate America today is generally handled in one of two ways—either on a mainframe or on a laser printer. Best practices for printing on a mainframe will be discussed later in the chapter. Generally speaking, laser jet printers are now considered the ideal way to print checks, assuming appropriate safeguards are incorporated in the process. For starters, no check stock is required. The best practices for storing check stock are explained in the section under that heading. Some companies use numbered safety paper—a recommended best practice. This paper is numbered and incorporates many safety features. Each piece of paper is sequentially numbered.

A log is kept of the sequentially numbered safety paper. By itself, the paper is worthless. However, with the right software, it can be turned into a valuable commodity—a negotiable check. When it comes time to print checks, the number of checks to be printed should be calculated. The safety paper is removed from the secure location, the first number of the sequentially numbered paper noted, and the checks printed. The last number of the sequentially numbered paper is noted. A calculation should be made, based on the beginning number, the number of checks printed, the ending number, and any ruined sheets of paper, to ascertain that no additional checks were printed. It is especially important to collect any allegedly damaged paper and destroy it.

The number of people who can print checks should be kept to a minimum. The person who prints the checks—usually by controlling the software through user IDs and passwords—should not have access to the check stock. Theoretically, when using a laser printer (which, by the way, is a regular laser printer), a check run can be had any time a manual check is requested. Each company must make a determination of whether this is desirable and if it wishes to pursue that course.

When checks are printed on a laser printer, the process usually includes use of a facsimile signature. Typically, this signature is included on a separate plate. Companies take different stances on this plate—some leave them in the printer, while others remove them. If the plate is left in the printer—or is an integral part of the machine—additional care must be taken with the printer. It probably should not be left out on the open floor. Although it is true that in order to actually print a check someone would need access to the software and would need to have a password and user ID, a printer with a facsimile plate could turn a plain piece of paper into a negotiable check. (Remember, checks don't have to be printed on special safety paper; it's just a good idea to do so.)

If preprinted check stock is used, a log similar to the one previously described should be kept. When it is time to run checks, one of the few approved staffers with access to the check stock closet should get the check stock out. Based on the number of checks that need to be run for each account, the appropriate number of checks should be removed. Some companies have so many different accounts that they end up using a cart to bring the appropriate number of checks for the different accounts to the computer room to be printed. The checks should not be stored in close proximity to the printer—it just makes it too easy for a thief to steal them. Typically, someone in Treasury or Accounting will bring the checks up to the Information Technology (IT) department to be run. This representative should watch while the checks are printed.

Since this type of check is typically of a continuous format, it is difficult, if not impossible, to rerun a check (in the same check run) if something goes wrong. When the checks are printed, notations should be made in the log regarding the first check number, the last check number, and the number of checks printed. Both the representative from Accounting (or Treasury) and IT should initial the log.

If a check prints off-center, jams, or has some other problem, it should be voided—either by writing *VOID* across the check in capital letters or by tearing off the MICR (magnetic ink character recognition) line. In any event, all damaged checks should be kept after voiding them. This is to ensure that the checks are actually voided and do not land in the hands of a crook. Also, make sure the appropriate entries are made to your accounting logs, or it will look like an uncashed check that should be turned over to the state as unclaimed property.

Some companies like to have two people present when checks are printed regardless of the methodology. In this case, both should calculate the number of checks used versus the check numbers and initial the log.

Periodically, the log used to verify check counts versus check paper used should be audited—and occasionally on a surprise basis.

At regular intervals, say once every two years, or if there is any significant change in activity (e.g., due to a merger or spin-off), a review of the frequency of check runs should be undertaken. As part of this process, an analysis of the number of rush checks (and the reasons for those requests) should be included. If too many rush checks are required, a company may want to increase the frequency of its check-printing process. If electronic payments continue to increase, many midsize companies may be able to cut back on the number of check runs they have each month. In fact, some will take this step in order to encourage vendors to sign up for electronic payments, which may be issued more frequently, if the company so desires.

Anyone involved in the check-printing process should have no responsibility for reconciling the company's bank accounts.

Once the checks are printed, they should be kept with great care until they are mailed. This means that if they are not mailed the same day they are printed (as they ideally should be), they need to be kept in a secure location. They should not be kept on the credenza of an executive who has to provide a second signature nor lying around the Accounts Payable department. More than one sticky-fingered employee or cleaning person has walked off with a check that did not belong to him or her.

Almost Best Practices: As you can see, especially if preprinted check stock is used, check printing can be a non–value-added, time-intensive task. Some companies choose to outsource this function to their banks. It adds little value and can cause a lot of trouble if not handled correctly.

Some would argue that including any check-printing data about anything other than laser printers in the "Best Practices" section is not appropriate and that printing continuous formatted checks on mainframes is not best practice. They might be correct. However, numerous companies still use continuous formatted checks, so they will be included in that section—at least for now.

Special Pointers for Accounts Payable: With a little bit of luck (okay, maybe a lot of luck) the check-printing function will diminish. For the last few years, the number of checks written has actually decreased. That decrease, at least for the titans of industry, has come through two best practices:

1. The use of p-cards and other practices to eliminate small-dollar invoices from the corporate landscape
2. The move toward electronic payments primarily through the ACH

Thus, check printing may become less of a problem at some point in the future.

Worst Practices: Worst practices include not taking the appropriate steps to guard both the check stock and the check-printing equipment. Several years ago an auditor noticed that his client had left the check-

printing machine out in the open with the signature plate in the machine. Luckily for his client, he was an honest man. To make his point, he printed a check for $1 million made out to himself and left it on the controller's desk with a little note. The controller got the message and made the appropriate changes in the check-printing policies and procedures. Most important, a company that does not exercise "reasonable care" in its check-printing procedures could open itself up to incur all losses associated with any check fraud. The worst practices include:

Inappropriate segregation of duties.

Not exercising reasonable care in the check-printing process.

Not maintaining a log to count the number of checks printed versus authorized.

Not storing printed checks carefully before mailing.

¶503 Check Signing

As part of the bill-paying process, checks must be signed. How this is done should depend largely on the up-front controls used to vet the invoice and the approval process. In reality, there is a second component––corporate culture. In theory, if up-front controls for approvals and duplicate-payment checking were perfect, there would be no need for a check to be signed by anything other than a machine. Very few companies, unfortunately, are in a position or are willing to let every payment fly through the invoice-processing cycle without some level of senior checking for high-dollar invoices. The definition of high-dollar invoices varies from company to company.

The information in this section assumes that the company is not using the check-signing process as a checkpoint to catch duplicate and inappropriate/unauthorized payments. If this is the case—and it is a really poor idea—then the company would not want to institute the practices designated in the "Best Practices" section but perhaps some hybrid as defined in the "Almost Best Practices" section.

The Board of Directors should authorize check signers. Alternatively, a senior-level executive who has been delegated by the board may give others signatory responsibilities. In either event, banks will require signature cards so that they can verify signatures on checks presented for payment. Do not assume from a bank's request for signature cards that it is checking signatures. Banks do not verify signatures. Occasionally, they will spot-check the signature on a check or pull a very-large-dollar check to verify the signature. The emphasis here is on the word *occasionally*. Any company that is counting on its bank to catch fraudulent checks will find itself with a load of bad checks unless it is using positive pay, which is discussed later in this chapter.

Best Practices: The selection of signers should depend on the number of checks that are manually signed as well as the personnel that will be available to actually sign the checks. Signers, however, should be of sufficient stature within the company and should check the documentation that accompanies the check for signature

Most companies put their top-level executives, such as the chief executive officer (CEO), chief financial officer (CFO), and so on, on their bank accounts as signers, even though these individuals rarely sign checks. They should rethink whether this is really necessary. When these officers sign the annual report, they should never use their actual signature. This is for the company's protection and the protection of the officers personally. In the early days of check fraud, thieves simply got a copy of the company's annual report to get a legitimate signature to use in their crooked check activities. Since these executives rarely sign checks, it is recommended that they not be included as signers on bank accounts.

Most companies today use a mechanized check-signing procedure that is integrated with the check-printing cycle. Depending on the dollar amount of the check, the mechanized signature can be the only signature or the first signature. If a mechanized process is used, the signature plate needs to be maintained with proper care and controls. This means it should be easily separated from the machine (computer) that prints the check, or, if it is not removed, the check-printing computer should be kept in a secure location with controlled access. The signature plate, or the machine with the plate in it, needs to be kept in a secure location with limited access. Many companies keep the signature plate used for facsimile signatures in a safe.

Even if up-front controls are airtight, many companies will require two signatures on checks over a certain level. The level will depend on the nature of the business and corporate culture. A smaller company might require the second signature for all checks over $25,000, while a Fortune 50 company might set that level at $1 million. The level reflects the company's comfort level with its invoice-processing controls.

There is a lot of debate over whether a warning should be printed on the checks indicating the level where two signatures are required. This is similar to the warning regarding the maximum dollar amount for which a check can be written. Some believe that putting a notice on the check stating, "Checks over $25,000 require two signatures" is a good idea as it alerts the teller of a possible fraud. Others rightly note that such indicator is likely to be of more use to a crook than to the teller. A crook noting such a warning will simply alter the check to no more than $24,999.

Most AP and Treasury groups at large companies keep a list of bank accounts and authorized signers. This is a good idea as long as proper care is taken with these reports. They should be limited in number and given only to those employees who need the information—definitely a need-to-know report. When the report is updated, the old reports should be collected and destroyed. Employees who receive the report should keep it inside their desks, not lying on top for easy access.

In no case should anyone who is an authorized signer on any account do bank account reconciliations.

When manual signatures are used on checks, the responsibility for getting the signatures (a truly thankless task) should be given to someone other than the person who prepares the checks.

When the check is given to the signer for signature, all the appropriate backup should be attached and the signer should verify that:

The check is actually for the invoices presented,
The appropriate approvals are in place,
The check is drawn on the correct account, and
The check is for the correct amount.

If the signer is not willing or capable of this verification process, he or she should not be an authorized signer. Periodically, spot-check checks automatically signed to verify quality control.

Almost Best Practices: When companies are not comfortable letting checks go without a senior-level review, the dollar amount where automated signing is acceptable is usually set quite low. Rather than fighting City Hall, AP can suggest that the level be gradually raised. As comfort is gained, the levels can be periodically raised.

Another way to address the issue of having too many checks is to look for ways to eliminate checks, especially checks for low-dollar purchases. Use of p-cards, electronic payments through the ACH, and direct deposit for travel and entertainment (T&E) reimbursements will help address the issue.

Special Pointers for Accounts Payable: Despite their best intentions, few authorized signers will actually go through the appropriate verification process before signing a check. The bulk of the responsibility for those tasks still lies with the AP staff, and if there is an error, it is rarely the signer who is held responsible.

Worst Practices: Worst practices include:

Signing checks with a rubber stamp. Although the ease with which checks can be signed with a rubber stamp is appealing to many, it has serious drawbacks. It is so easy for a thief to copy a signature made with a rubber stamp that a company that uses a rubber stamp to sign its checks is not considered to be using ordinary care. The implications of not using ordinary care mean that should any check fraud happen, the company would be liable for 100 percent of the loss.

Some companies, thinking they are improving controls, set the dollar level at which hand signatures are required very low. When an executive is presented with many checks to sign at one time, it is unlikely that he will give each an adequate review. Rather than set the dollar level low, it is far better to set it higher, and have fewer checks representing higher dollar invoices undergo a thorough review.

¶504 Check Stock Storage

Blank checks may look innocuous enough, but in the wrong hands they can cause a lot of damage. A thief, disgruntled employee, or even just an inexperienced staffer can cause untold trouble by misusing company checks. In the past, banks ate the losses associated with check fraud. This is no longer the case. They just can't afford these hits to their bottom line. Often, this is an area that is overlooked—no one gives it much thought. However, with all the attention of the recent accounting scandals, the enactment of the Sarbanes-Oxley Act, and the new emphasis on internal controls, how a company stores its checks is likely to come under increased scrutiny.

Best Practices: In the "Check Printing" section, there was a discussion of both laser checks printed on safety paper and preprinted checks. While this discussion does cover both types, it applies to preprinted checks to a larger degree, as that is where the real risk lies.

Checks should be stored in a secure, locked location.

Access to the check stock should be severely limited.

The closet should be reinforced—and not of the type that a crook could easily hack into.

The lock on the door should be substantial and not easily picked with a hairpin or clothes hanger.

Ideally, the check storage closet should not be in close proximity to the printer. If someone breaks in, especially on a long weekend, don't make it too easy for him or her.

Sufficient segregation of duties should be incorporated into the various tasks associated with the check production cycle, so the individuals with access to the check storage closet do not also have the authority to print checks. Clearly, anyone with access to the check storage closet should not be responsible for the reconciliation of the company's bank accounts.

Almost Best Practices: When it comes to storing of checks, there is not much give-and-take. It is something that a company really needs to do right, because the consequences of doing it wrong are too great. Therefore, best practices should be employed.

Special Pointers for Accounts Payable: The check stock storage issue is likely to be a touchy issue at some smaller and midsize companies. If the check stock or a spare checkbook has always been kept in the assistant controller's office, he or she may be insulted at the suggestion that it really should be moved to a more secure location. This is an internal controls issue, and if necessary, the auditors should be asked to weigh in on the issue.

Worst Practices: Worst practices include:

Keeping a spare checkbook around, in someone's desk, for those after-hour emergency situations.

Keeping checks in the bottom drawer of a filing cabinet, especially if that cabinet is often open and unattended for long periods of time.

Storing the check printer (and signature plate) in the same locked room as the check stock.

Not adequately segregating duties when it comes to check printing, storage, and the reconciliation of bank accounts.

¶505 Distribution of Checks

Once a check is printed and signed, it has to get in the hands of the payee. The normal way that this is handled is to mail the check to the payee. In fact, some may wonder why there is a separate section for this topic. The answer is that sometimes the person requesting the check will request that the check be returned to him or her for final distribution. Typically, there are three reasons that this request is made:

1. The requestor wants to make sure that the check is mailed correctly.

2. The requestor is a salesperson who wants to deliver the check to the customer and try and pick up another order at the same time.

3. The requestor has some other business relationship with the payee and wants to solidify that relationship.

While the reasons may appear reasonable at first glance, they are overridden by several other concerns, including the following:

It is extremely inefficient and time-consuming to return checks to the requestor. Few people outside Accounts Payable realize how disruptive the practice is.

The door for employee fraud is opened wide whenever checks are returned to anyone other than the payee.

Checks returned to the requestors are sometimes lost, misplaced, or not delivered for a long time, often resulting in duplicate payments.

Best Practices: When an invoice is approved for payment, the invoice should have a mailing address on it. Additionally, this address should match the pay-to address in the master vendor file. Any variation from this should be investigated because it may be the first sign that something is amiss. Under all but the most extenuating circumstances, checks should be mailed.

When checks are mailed, care should be taken regarding when and how this is done. Checks should be sealed in envelopes and delivered either straight to the post office or to the mailroom at the end of the day.

If checks are delivered to the mailroom, they should not be left out in the open where anyone walking by can see them and easily steal one. This is especially true if temporary employees are frequently used.

Similarly, thought should be given as to whether a window envelope should be used. While window envelopes simplify the mailing of checks, they are also a red flag for a crook looking for checks to steal. Rarely are checks mailed in anything other than window envelopes.

Additionally, if one-part sealers (those multipart forms that contain the check) are used, extra care should be taken in the mailing procedures. Again, they are often a red flag to crooks looking for checks.

Almost Best Practices: Sometimes, the corporate culture or the nature of the business will require the hand delivery of checks, either to company employees or to the customers' representatives. In these cases, to avoid disrupting the AP department too much, the pickup time should be limited to certain days and hours.

A log should be kept for checks not mailed. Each time a check is picked up, the following information should be noted in the log:

Check number
Payee
Dollar amount
Date the check was issued
Date the check was picked up
Name of the person picking the check up

The person picking up the check should sign each of the entries. Of course, the list of who can pick up checks should also be limited.

Although companies often tolerate the practice of not mailing checks directly to the payee, it should be discouraged. Anytime someone requests that a check be returned, ask why he or she needs it and then point out the advantages of not returning the check.

Requiring an extra level of approval for returned checks will sometimes put a damper on these requests. Paying customers electronically eliminates this issue!

Special Pointers for Accounts Payable: If the company tolerates the practice of individuals picking up checks, there will be occasions when AP will have to make these checks available outside of the preset hours. This practice should be discouraged as much as possible.

If checks are to be regularly segregated for delivery rather than mailing, firm policies and procedures should be written to govern the process.

Worst Practices: Worst practices include the returning of checks to anyone other than the payee, especially if the person who approved the invoice for payment is the individual to whom the check is returned.

Although circumstances may dictate the issuing of a manual check and returning it to the individual who approved the payment, these should be limited.

¶506 Check Fraud

Although no one knows the true level of check fraud, most experts estimate that it is at least a $10 billion-a-year business. In years gone by, banks would eat the losses associated with check fraud for their corporate clients. This has become prohibitively expensive, and banks are no longer willing or able to absorb these often unnecessary expenses. Changes to the Uniform Commercial Code (UCC) have introduced the concepts of reasonable care and comparative culpability.

In plain English this means the person in the best position to prevent the crime will be held responsible. This is done on a pro-rata basis, although there are some things that companies do that place the responsibility 100 percent on their plate. A simple example of this is using a rubber stamp (not a facsimile signer) to sign checks and not keeping check stock in a secure location.

Those who are interested in reading the statutes that cover payment fraud–related issues can refer to:

UCC3 for ordinary care
UCC4 for reasonable notification
UCC4A for acceptable security procedures
Regulation CC for shortened return/hold times
The National Automated Clearing House Association (NACHA) for unauthorized entries return
Certain state statutes

The states have also changed their laws so that companies that fail to exercise "reasonable care" are now allocated the losses associated with check fraud.

Best Practices: While at first blush making all payments electronically might seem to eliminate the problem, it is not practical in today's environment. Numerous companies are not able to take this step, and even more limiting is the fact that a number of their customers are not yet ready to accept payments electronically.

A reasonable best practice for companies is to move as many of their customers to an electronic payment mechanism as possible. In most instances this will require a renegotiation of the payment terms to make the transaction float neutral. If a customer sees the move toward electronic payments as an attempt on the part of the vendor to improve its position, it is unlikely to agree to pay electronically. In a float-neutral situation, both parties still benefit from improved efficiencies and reduced costs.

In addition to positive pay discussed below, companies also need to focus on the check itself. The check should contain some (but not necessarily all) of the following security features:

Watermarks. Watermarks are subtle designs of a logo or other image. Designed to foil copiers and scanners that operate by imaging at right angles (90 degrees), watermarks are viewed by holding a check at a 45-degree angle.

Microprinting. A word or a phrase is printed on the check so small that to the eye it appears as a solid line. When magnified or viewed closely, the word or phrase will become apparent. Copiers and scanners can't reproduce at this level of detail, so microprinting when copied will appear as a solid line.

Laid lines. Laid lines are unevenly spaced lines that appear on the back of a check and are part of the check paper. This design makes it difficult to cut and paste information such as payee name and dollar amount without detection.

Reactive safety paper. This paper combats erasure and chemical alteration by "bleeding" when a forger tries to erase or chemically alter information on the check, leaving the check discolored.

Special inks. These are highly reactive inks that discolor when they come into contact with erasure chemical solvents.

Color prismatic printing. This type of printing creates a multicolor pantograph background that is extremely difficult to duplicate when using a color copier or scanner.

Special borders. These borders on the check have intricate designs that, if copied, become distorted images.

Warning bands. Warning bands describe the security features present on a check. These bands alert bank tellers or store clerks to inspect the check before accepting it. They may also act as a deterrent to criminals.

Thermochromic inks. These are special colored inks that are sensitive to human touch and, when activated, either change color or disappear.

Toner grip. This is a special coating on the check paper that provides maximum adhesion of the MICR toner to the check paper. This helps prevent the alteration of payee or dollar amount by making erasure or removal of information more difficult.

Preprinted check stock should not be ordered from a printer but rather printed on safety paper as needed. This means that all the controls surrounding check stock become irrelevant because the only thing the company has ordered is blank paper. The appropriate controls need to be with the software and hardware used to print the checks.

Almost Best Practices: Not every company is willing or able to walk away from preprinted check stock. If the company does use preprinted check stock, appropriate care must be taken to ensure that checks are stored under lock and key and access to the storage area is limited. Additionally, anyone who is an authorized signer or has access to the safe where the signature plates for the check-signing machine (or computer) are kept should not have access to the check stock.

Special Pointers for Accounts Payable: Some companies are very attached to preprinted checks. It is up to the AP executives at these companies to make sure that adequate controls are used with regard to the check stock. Occasionally, organizations will come to the conclusion that because of the move to electronic payments, they can let their guard down when it comes to protections against check fraud. This can lead to disaster. Recent statistics from the Association of Financial Professionals reveal that check fraud is still the most common type of attempted payment fraud. The emphasis is on the word *attempted*. If the proper precautions are taken, these crooks won't be successful. Let up your guard and you'll find they are walking off with your organization's money.

Worst Practices: Worst practices include:

Not using positive pay.

Not keeping checks in a secure location.

Not incorporating fraud prevention features in check stock.

Using a rubber stamp to sign checks.

¶507 Use of Payee Name Positive Pay

A few years ago, the use of positive pay was seen as a leading-edge technique to limit check fraud. Today, it should be part of the payment process at every company. Some think that in a few short years not using positive pay will be seen as not exercising reasonable care. Positive pay is a service offered by most banks. As part of the service, companies transmit to their banks their check issuance file each time checks are written. The file contains a list of check numbers and dollar amounts. When a check is presented for payment, it is matched against the file. If there is a match, the check is honored and the check number removed from the file. It there is no match, the check is handled according to the preset instructions from the company. This may mean automatically rejecting the item, but more likely it means notifying the company and giving it a few hours to send instructions on how the item should be handled. What has been described so far is the basic positive pay service.

A more recent innovation in the area of positive pay is the development of a more advanced product called payee name positive pay. As you might expect, this includes the payee's name along with the check number and dollar amount in the file sent to the bank. Companies should contact their bankers for the details of the products offered.

While use of the positive pay service is definitely a best practice, some companies have trouble transmitting an issue tape to the bank. For these companies, reverse positive pay is a reasonable option, while they try and alleviate the situation that prevents them from giving the bank a check issuance tape. In this case the bank will transmit a file to the company containing all the checks clearing against the company's account that morning. The company is then responsible for reviewing the information within a few hours and contacting the bank about any that should not be honored. Alternatively, the company can make arrangements with the bank that it honor all checks unless notified.

Best Practice: Use payee name positive pay wherever available. This is your best protection against check fraud.

Almost Best Practice: Use positive pay, if payee name positive pay is not available. If the organization does not have the ability to create a positive pay file, then reverse positive pay is the best option. Basically, this requires the organization to verify checks clearing each day. It is the organization's responsibility to notify the bank of any unauthorized checks. If it forgets or someone is out, the bank is off the hook, if there is a check fraud. Verifying on a daily basis effectively means the task of bank reconciliations is done daily rather than monthly. Additionally, as will be discussed in the chapter on fraud prevention, daily bank reconciliations are recommended as a way of guarding against unauthorized ACH transactions.

Special Pointers for Accounts Payable: Accounts Payable often has a hard time convincing management that positive pay should be used. Don't let this issue drop. While positive pay or payee name positive pay will protect your organization against check fraud, which is all it will protect against. It will not protect against other types of payment fraud. Thus, it is imperative that other steps be taken in the battle against payment fraud, with positive pay being just one weapon in your arsenal of defense against the fraudsters trying to defraud your organization.

Worst Practice: Not using any type of positive pay at all.

Review Questions

18. When it comes to making payments, which of the following is a best practice approach?
    a. Pay everything by check.
    b. Encourage vendors to accept electronic payments.
    c. Always pay by check unless requested otherwise.
    d. Refuse to pay by check.

19. Which of the following actions should be taken when using preprinted check stock?
    a. A log should be kept comparing the number of checks printed with the check numbers used.
    b. Check stock should be kept near the printer for ease of use.
    c. Damaged checks should be thrown away.
    d. Checks should be signed as they are printed by the person printing the checks.

20. Who should authorize check signers in the organization?
    a. The accounts payable manager
    b. The treasurer
    c. The Board of Directors
    d. No one

21. When it comes to check storage, which of the following is ***not*** a best practice?
    a. Storing checks in a secure locked location
    b. Keeping a few emergency checks in a desk drawer
    c. Limiting access to check stock
    d. Using a strong lock on the door to the closet where checks are stored

22. What is the best time to take checks to the mailroom for final delivery to the post office?
    a. Whenever they are ready to go
    b. First thing in the morning
    c. Right before mail is taken to the post office
    d. It really doesn't matter.

¶600 ACH (Electronic Payments)

Learning Objectives

Upon completion of this chapter, you will be able to:

Understand the benefit of paying electronically

Develop a process to weed out fraudulent change of bank account requests

Construct a process to provide vendors with remittance information when paying electronically

Electronic payments have long been the norm in parts of the world outside the United States. Now, organizations of all sizes and types within the United States are starting to take advantage of electronic payments, also referred to as ACH payments or direct payments, to pay their vendors. Most organizations rely on the ACH for their direct deposit of payroll payments. Now, they are taking that approach one step further, using the ACH to pay vendors. The terminology of *direct payment* is a nod toward direct deposit of payroll. In this chapter, best practices related to the following are discussed:

Approach to Paying Electronically
Converting Vendors to ACH Payments
Handling Change of Bank Account Requests
Convincing Vendors to Convert
Handling Remittance Information

¶601 Approach to Paying Electronically

By now, you probably realize this author strongly believes in paying electronically instead of using paper checks. The issue is how to get from point A (the paper check world) to point B (an electronic payment arena). The obvious answer is that you can't do it all at once. Many of your vendors won't have the ability to accept electronic payments and apply cash correctly, and your own staff is probably not capable of converting the entire vendor base in one fell swoop.

Keep in mind that as the business and accounts payable world is changing, one of the big areas is the use of technology and automation in accounts payable. This includes paying electronically. Even if you don't believe your organization will ever make this move, you may find yourself forced into the electronic payment world when a large supplier dictates electronic payments or taking their business elsewhere. It's the wave of the future, so stop trying to fight City Hall.

Best Practice: Consider moving towards making electronic payments, if you have not already started, and if you have, considered increasing the number of vendors paid in this manner. Not only is it more efficient for the accounts payable staff, it is less costly.

The first step in moving into the electronic payment world is getting your own house in order. This means making the necessary changes to procedures and systems to allow electronic payments to be made. It also means getting everyone on board in-house. This would include both management and the purchasing staff. By explaining the benefits to them, they are less likely to object and might even become missionaries advocating for electronic payments instead of paper checks.

Almost Best Practice: If you are not ready to make a full-court press into the electronic payment world, consider at least paying electronically those vendors who request such payments. This will enable you to dip your foot into the electronic payment waters without making a full-fledged commitment. It is also likely that the vendor will understand if there are a few snafus in the beginning. This is a great way to get started. Once you have been successful with a few electronic payments, you'll look for ways to increase your participation.

Special Pointers for Accounts Payable: Be aware that there is a cash flow impact associated with making electronic payments. Let me give you a simple example. If you are paying vendors with paper checks that are typically mailed on Fridays, you can probably predict with great certainty when most will clear the

bank. You might end up with 10 percent clearing on Monday, 50 percent clearing on Tuesday, 30 percent clearing on Wednesday, and the rest trailing in over the next few days. Your cash forecasting folks probably have this built into their cash flow model.

Now, if you move to electronic payments, 100 percent of your transactions will clear on Monday. This shouldn't deter you from making them, but you do need to factor this into the process.

There are two ways to deal with this issue. The first is to renegotiate payment terms with your vendors to make the transactions float neutral. This typically means adding one or two days to the payment terms. However, this is not always possible. If the vendor doesn't really care whether it is paid electronically, you don't have as much leverage. Despite the vendor's refusal to negotiate terms, it is still recommended you go the electronic payment route. That's because even without the extra days, you are still better off paying electronically than with a paper check.

Worst Practice: Absolutely refusing to pay anyone electronically.

¶602 Converting Vendors to ACH Payments

There's a bit of work involved converting vendors from paper checks to receiving ACH payments. Deciding that you will pay this way is just the first step.

Best Practice: Develop a systematized approach to converting vendors to electronic payments. Start with a beta or test group. This might be composed of transactions between various company entities, or it might be trusted vendors who won't complain if the payments don't go as planned the first time out. Don't overlook those vendors clamoring to be paid electronically. All these groups will be less critical should something go wrong than your vendor population at large. You can also try a second beta group consisting of employees being reimbursed for travel and entertainment expenses.

Once you've got your beta group and run a few payments through, review what happened and adjust your procedures to address any rough spots. When you are confident that you have everything working well, it's time to roll out your program to your entire vendor base. But don't do it all at once. One company sent letters to all their vendors expecting a tepid response. When over 25 percent responded affirmatively, they could not handle the demand and ended up hurting their relations with vendors who were not accommodated. Figure out how many vendors your staff can comfortably convert and make your pitch accordingly. Once you have the first group of positive respondents converted completely, send out the solicitation to your next group. Proceed like this until you have contacted all your vendors at least once.

If your process takes more than six months, when you finish, start again approaching those vendors who turned you down the first time.

Almost Best Practice: As above, pay only those who request electronic payments until you are comfortable with the process. Then go full steam ahead, approaching all your vendors systematically, as described above.

Special Pointers for Accounts Payable: No matter how hard you try, you will have some vendors who just refuse to convert. Consider paying less frequently with checks than electronically. For example, you might make electronic payments three times a week but only have one check run each week, or even every two weeks. Additionally, insist that all rush payments be made using electronic payments. Sometimes it just takes one payment for the vendor to see the light.

Worst Practice: Refusing to pay any vendor electronically.

¶603 Handling Change of Bank Account Requests

Organizations change bank accounts all the time for a variety of reasons. Many times the old account is closed. Sometimes the company has changed its legal structure; sometimes it has changed banks. Occasionally, a fraud has occurred necessitating the change of account. Whatever the reason, when the change is made, if the organization has been receiving payments electronically, it notifies its customers of its new account. Most often, notification of this change comes in the form of an e-mail.

Unfortunately, crooks, often quite sophisticated in the use of the Internet, realize this is a potential gold mine. They spend a bit of time analyzing potential targets and creating quite legitimate-looking e-mails.

These e-mails purport to come from the vendor, notifying customers of a change in the account where payments are being sent. As you might expect, the new bank account is one they control. Once money is sent to the account, it is quickly transferred out of the country, making recovery difficult. Regrettably, if your company falls victim to such an e-mail it will still be on the hook for the payment.

Don't be fooled because the e-mail either looks legitimate or looks like it came from the vendor's e-mail account. Really smart IT folks can make the message look like it originated at the vendor's ISP.

Best Practice: An emerging practice that completely takes the onus off the customer is the use of automated self-service vendor portals, where the vendor is responsible for inputting its data, including bank account information for electronic payments *and* any changes to that information. This removes the onus from the customers. However, as this is being written, most organizations do not have such a portal and therefore it is imperative that they do an independent verification of the request. This means contacting the vendor using information already on file to verify the change was a legitimate request. This also means regularly updating vendor contact information, something few companies do at this time.

Almost Best Practice: A few organizations now require that anyone requesting such a change supply not only the new bank account number but the old bank account number as well. This makes it much more difficult, but not impossible, for a crook to perpetrate this type of fraud.

Special Pointers for Accounts Payable: This type of fraud is expected to grow in the coming years. It is a variant on the "change of remit-to address" letters crooks sometimes send. Those too should be verified, again using information you have on hand, not information included with the request.

Worst Practice: Just following the instructions in the e-mail or the letter without doing any verification that the request is legitimate. Equally bad is calling the phone number provided in the e-mail to verify the request. If it is a phony request, the person who answers the phone at the number provided will verify it is legitimate, when of course it is not. This is why keeping current contact information is so important.

¶604 Convincing Vendors to Convert

Converting vendors to ACH payments unfortunately takes a lot more than just deciding this is what you want to do. Unfortunately, you also have to convince your vendors that this is a good approach for them as well. Some will immediately see the benefit, while others will drag their feet. But paper checks are just inefficient and best-practice companies everywhere are looking for ways to minimize the number they must issue. What's more, outside the United States, most companies use very few checks. Other countries have relied on electronic payments for eons—and they work!

Best Practice: Actively work to convert vendors to your electronic payment program. You can do many things to encourage this conversion, including:

Explaining the benefits to them (not to you—they don't really care about that)
Paying more frequently with electronic payments than paper checks
Reducing the number of check runs
Paying electronically the day before you release paper checks
Keeping track of those vendors who seem to be on the fence and re-soliciting them every six months

Almost Best Practice: Paying electronically only those vendors who request electronic payments. While this is a good way to dip your feet in the electronic payment waters and get used to the process, it should be done only for a short period of time. Then, the hope is your organization will realize the benefits of paying electronically and flip into the best practice mode.

Special Pointers for Accounts Payable: If you are very serious about converting as many vendors as possible, insist that all rush payments be made electronically. There are two benefits to this approach. First, it is easier for accounts payable and removes the request for the return of the check to the requisitioner, which happens frequently with rush or ASAP payments. And second, it introduces the vendor to the concept of accepting electronic payments. Many will find they like getting paid this way and sign up to receive payments in this manner in the future.

Don't assume you'll immediately need fewer staff as you get rid of paper checks. That's true eventually, especially if you have a particularly manual process and are getting hand signatures on more than a few

checks. But it will take some effort to handle the conversion, so initially you will not have staff to redeploy to more value-added tasks. However, eventually when you've gotten over the hump of converting most of the suppliers who are willing to take electronic payments, you will be able to free up some of your resources.
Worst Practice: Refusing to pay any vendors electronically. This sticking-your-head-in-the-sand approach is not likely to work for long as more and more organizations see the benefits of being paid electronically. Eventually, every organization will have to do this as 800-pound-gorilla suppliers demand electronic payment. So, why fight this losing battle?

¶605 Handling Remittance Information

On the face of it, you'd think every supplier would be clamoring for electronic payments. Yet, some refuse to accept them. While at first this seems counterintuitive, there is a good reason for this reluctance. Their cash application folks have difficulty applying cash without that all-important remittance information. If this hurdle can be overcome, many are all too happy to get on board with accepting electronic payments.
Best Practice: Create a separate e-mail with all the remittance information and e-mail it to the appropriate accounts receivable or cash application person at your vendors. This will provide them the information needed to apply cash correctly and should remove what is hopefully the last obstacle to their accepting electronic payments. If you are able to provide this information a day or two in advance of the payment, it might also help with their short-term cash forecasting—another side benefit.
Almost Best Practice: Mailing the remittance information after the fact. While this is better than nothing, it does take away some of the cost savings associated with the move to electronic payments.
Special Pointers for Accounts Payable: A side benefit of this approach is that you will be forced to keep updated information for the accounts receivable staff. This is something that is recommended as part of a fraud prevention program to help protect the organization against certain types of electronic payment fraud. By collecting the current contact information for remittance advices, you will be one step ahead on that front in your fraud prevention/detection initiatives.
Worst Practice: Ignoring the issue of remittance advices. Even if your vendor is willing to accept payments electronically without remittance information, you are putting your organization at the mercy of the vendor's cash application person. Typically, without other instructions, the vendor will apply whatever cash comes in to the oldest outstanding invoice. This may not be what you intended. For example, it could be a disputed invoice that you have no intention of paying. Hence, it is critical that remittance information be included so the supplier knows precisely what you intended to pay with the payment in question.

Review Questions

23. What is the *worst* practice when it comes to making electronic payments?
    a. Refusing to pay anyone electronically
    b. Insisting on paying electronically
    c. Only paying those who request electronic payment electronically
    d. Making all rush payment requests with electronic payments

24. What is the best approach when converting vendors to accepting electronic payments?
    a. Send a mass mailing to all vendors.
    b. Develop a systematized approach to converting all vendors.
    c. Only convert those who ask.
    d. Insist that they all start accepting electronic payments immediately.

25. When you receive an e-mail asking you to change the bank account where you are sending a vendor payment, which is the recommended action?
    a. Start sending payments to the new account.
    b. Verify the request by responding to the e-mail.
    c. Verify the request by calling a phone number provided in the e-mail.
    d. Verify the request by calling a phone number you already have in your files.

26. Which of the following practices will not help convince reluctant vendors to accept electronic payments?
    a. Asking for extended payment terms
    b. Paying more frequently with electronic payments
    c. Explaining the benefits they will accrue due to their acceptance of electronic payments
    d. Paying electronically a day or two before paper checks are released

¶700 An Effective P-card Program

Learning Objectives:

Upon completion of this chapter, you will be able to:

Craft an operative p-card policy

Identify places where rebates on p-cards can be increased

Develop strong controls in a p-card program

P-cards, also sometimes referred to as *purchase cards*, *corporate procurement cards*, or simply *procurement cards*, are a great tool for organizations looking to get rid of small-dollar invoices in accounts payable. They also can serve to make the procurement process more efficient. However, if proper controls are not incorporated into the p-card program, payment problems can creep in.

There is one other huge advantage in using p-cards. For the most part, the card issuer is responsible for issuing Form 1099s for payments made on p-cards. This is a recent change to the US tax code and relieves the organization of filing that information. In the past, this was a huge stumbling block for US companies. It no longer should be a consideration. In fact, if you have a vendor who is balking at providing Form W-9 information and it accepts credit cards, considering paying it this way and eliminating the problem. In this chapter, best practices related to the following are discussed:

Designing a Best Practice P-Card Program
Setting Strong Internal Controls in Your P-card Program
Increasing Usage of the P-card in Your Organization
Setting Attractive Payment Terms
Increasing Rebates Based on Card Usage
Employees Using Cards Deceitfully for Personal Gain

¶701 Designing a Best Practice P-Card Program

An effective p-card program needs to be planned out very carefully. Although most people understand what a p-card is, not everyone realizes that the p-card program needs to be well thought out and the mechanics of how it will work spelled out to employees. Assuming that because your employees know how to use credit cards, they will know to use the p-card is likely to lead to big-time headaches. Because when it comes to procurement cards, there's a lot more to the process than simply handing a clerk in a store your card and saying, "charge it." To achieve a best practice p-card operation, you need to lay a strong foundation at the beginning. And that means the program must be well designed.

Best Practices: Each organization with a p-card program needs a formal written policy that is shared with all affected parties. This means not only the people who have and use the cards, but also their admins who might do the necessary reporting. Do not leave out any details assuming your employees will know something. You will learn the hard way that there a few who don't have the same knowledge base.

Your policy should address:

Who should have a card, based on job responsibilities not title
When the card *must* be used
Where the card *can* be used
List of preferred suppliers, where applicable
Specific instances where the card should *not* be used (if there are any)
Transaction limits—both dollar wise and number per day (if any)
Spending limits—daily, if any, and monthly
Detailed procedural instructions for end-users, including but not limited to card activation, card training, reporting, handling of receipts, record retention, the approval process reporting, handling of lost or stolen cards, and consequences for misuse

Of great importance is the use of a cardholder agreement, which details the end-user's responsibilities. It should also clearly spell out the consequences of misuse, including the fact that the employee may be fired if the misuse is deemed egregious or of a fraudulent nature. This agreement should be signed before the cardholder is given the card. The cardholder should also be required to undergo training on proper use of the card, as well as his or her reporting responsibilities.

Like other AP policies, the p-card policy should be updated periodically, ideally whenever a change is made or, at a minimum, once every year. These changes should be reflected in the policy and communicated to all affected employees. It can be published on the Internet or intranet site for easy access by all employees.

Almost Best Practice: It is a good idea to limit the payment vehicles for each vendor to one particular type. This prevents duplicate payments from occurring because, for example, one was made using a check and another using a p-card. While this works well in theory, in practice it is not smooth sailing and may not be possible. For example, a cardholder may need to purchase something that is over his or her monthly limit. Thus, in reality it will often be necessary to break the principle of one payment approach per vendor. However, wherever a p-card can be used, it should be.

Special Pointers for Accounts Payable: Occasionally, you will have employees who refuse to use the card. If they cannot be turned around, request the return of their card. It is not a good practice to have inactive cards lying around. Folks should either use them or return them.

Cards should be retrieved from departing employees. This includes those who left the company on their own to take new jobs as well as those who were terminated for poor performance. When the cards are returned, immediately cancel them with the bank. If HR does not notify the card administrator when employees leave, periodically run reports showing cards with no activity. Investigate all entries on the report to find out if they have left the company or are simply not using the card. Terminate the cards of those who are no longer employed by the company. Talk to those who are not using the card. Sometimes a little extra training is all that's needed to get the employee to use the card. If not, and they still refuse to use the card, terminate the card.

Worst Practices:

Not getting cards back from departing employees.

Not regularly updating your p-card policy and procedures manual.

Not sharing the p-card policy with all affected employees.

¶702 Setting Strong Internal Controls in Your P-card Program

Handled properly, p-cards are one of the lowest risk payment vehicles any organization can use. If you follow the guidelines listed below, your potential for loss due to misuse or fraud will be minimal. This is important because one of the most frequent objections to p-card use is the concern that the cards will not be used properly and put the company at risk. In actuality, there has been little reported improper card use, and the risk objection can be easily overcome by ensuring that the proper controls are in place.

Best Practice: There are a number of best practices every organization should use to ensure strong internal controls in your p-card program. Let's take a look at a few.

Establish card policies and procedures for all employees. When a procurement card program is begun, detailed guidelines and procedures should be provided to all affected employees, including the admins who may do the reporting for their bosses. They are often forgotten.

Limit the dollar amount of each transaction for each employee. This amount will vary depending on the person's job needs. These limits can always be changed if it is determined that the original level was not high enough. They can also be adjusted seasonally, if that is required.

Limit the dollar amount that can be spent each month by each employee. In addition to the dollar amount each employee can spend per transaction, it is also possible to set up a monthly constraint. This, too, can vary by employee and area of responsibility. This control device limits the amount of risk a company has with the card. In extreme examples, these can be set as low as $100.

Use Merchant Category Code (MCC) blocks. Companies concerned that an employee will take the card and go shopping for a new flat-screen TV or take a trip to Hawaii can use MCC block. By disallowing charges at certain MCC codes, a company mitigates this issue. Of course, this matter can be resolved by the dollar limits placed on the employee for each transaction and for each month.

Make a monthly review of all charge card statements mandatory and require a supervisor's signature on each statement. This after-the-fact review will uncover any spending that might be slightly off base. It also assures management that the proper oversight is being given to all expenditures, and improper spending not otherwise detected won't turn up. And hopefully, it puts managers on notice that they are expected to closely review the expenditures made by their subordinates.

Make everyone aware that from time to time senior management and more likely internal audit will come in and review the statements for the entire company or any one department or individual.

Set guidelines for where the card can be used. This will guard against the card being used inappropriately. You might also include MCC blocks where you don't want it used—ever.

Institute strong card cancellation procedures. This puts everyone on notice that the card can be revoked at any time the corporation sees fit. This is especially important in the instance of employee termination. Regardless of the cause, the AP manager will want the ability to immediately cancel the card when an employee leaves the organization.

Almost Best Practice: As a bare minimum control, dollar limits should be set on the cards given each employee. This information needs to be clearly communicated to the employees so there is no misunderstanding.

Special Pointers for Accounts Payable: No matter how hard you work to establish strong controls over the program, there will always be exceptions that don't fit into the big picture. Whenever those loopholes appear, work to adjust the procedures so the controls prevent misuse or inappropriate use.

There is also something to be aware of regarding MCC blocks. Many organizations rightly put blocks on casinos. You can certainly understand the rationale for that. However, occasionally you'll have an employee who is attending a conference that is held at a casino. If you've combined your travel and entertainment card and your p-card programs and have put an MCC block on for casinos, the employee who goes to check into the hotel at the casino is in for a nasty surprise when he or she presents the credit card. It will be rejected. This is easy enough to get around, assuming you know about it. Simply remove the block for that one employee for the period of time he or she is at the conference. As soon as the conference is over, slap the MCC block for casinos back on the card.

Worst Practices: Worst practices include:

Having no controls built into the program.

Allowing employees to use the card as they see fit.

Not getting cards back from departing employees.

¶703 Increasing Usage of the P-card in Your Organization

P-cards are attractive to companies for a number of reasons, including the fact that they get small-dollar invoices out of the invoice process, ultimately making the accounts payable department more efficient. As rebates become more commonplace, even for midsize programs, the drive to increase usage within the organization intensifies. But, this doesn't mean haphazardly putting all possible purchases on the card. Rather, a more reasoned approach needs to be taken.

Best Practice: Whether you are looking to increase usage because you want a higher rebate or you are simply looking to get some of those low-dollar invoices out of your invoice processing cycle is irrelevant. The techniques are the same. A few savvy companies have realized they can also improve their cash flow by using p-cards. They simply wait until the end of the payment cycle and then instead of paying with a check or ACH, they call up and provide their credit card information.

Here are a few ways best practice organizations have increased p-card usage in their organizations.

Make sure everyone who has a card is using it every place they should be.

Mandate the use; don't give employees an option.

Educate every cardholder about all the potential opportunities to use the p-card.
Increase the number of merchants in the p-card program
Look for new opportunities to use the card. This can include things like paying for subscriptions, office supplies, and so on.
Offer cards to all employees who make frequent small-dollar purchases.
Whenever an invoice comes in that could have been paid for with a p-card, send it back to the approver asking for it be paid for with the p-card.
With management support, refuse to pay any invoice with a check for which a p-card could be used.
Consider merging your travel card and your fuel card into your p-card program.

Almost Best Practice: None.
Special Pointers for Accounts Payable: Before you take any of the more aggressive steps mentioned above, make sure management supports the initiative.
Worst Practice: Not growing your program intelligently.

¶704 Setting Attractive Payment Terms

How the corporate p-card bill is paid can affect a company's bottom line. Just as companies routinely negotiate payment terms with other suppliers, they should also handle their p-card obligations similarly. If the program is effective, the bill is likely to be one of a company's larger obligations. But realize that getting longer payment terms could have some ramifications. You may earn fewer rebates because of your longer payment terms. This is an issue each organization has to decide for itself. They need to determine which is more important: longer payment terms or higher rebates.
Best Practice: Your corporate credit card bill is very different than your personal credit card bill, and not just because it is for a much larger amount of money. In most cases, without further action, payment on the corporate procurement card bill is expected within 7 days of receipt of the bill.

A number of companies have succeeded in getting these terms extended to 14 and even 21 days. If you are a net borrower, you may be able to reduce your borrowing expenses by getting the payment delayed a week or two each month. If you are a net investor, you may be able to increase your investment returns. However, you'll need to weigh that against any potential reduction in rebates. This is especially true when short-term investment rates are low.
Almost Best Practice: None.
Special Pointers for Accounts Payable: If the program is not large enough, the issuer may be reluctant to negotiate payment terms. If that happens, revisit the issue when the program expands. At lower levels, it is unlikely that the issuer will be receptive to your overtures—both on this issue and on the matter of rebates.
Worst Practice: Paying the bill before the due date.

¶705 Increasing Rebates Based on Card Usage

Rebates have become a hot topic in the p-card world. Once only whispered about, they are now discussed openly. Companies that spend a significant amount of money on their p-cards have found that card issuers will compete for their business by offering rebates, based on the level of purchases. For organizations struggling with cash-flow issues or ravaged by several years of a business downturn, this is manna from heaven. What's more, you used to need a million dollars or more per month of spend on the card to qualify for the rebates. But that figure has dropped drastically in recent years.

What companies do with their rebate money is interesting. Some use it to finance projects they could not get funding for through normal budget channels. Others return it to the departments making the purchases, on a pro-rata basis.
Best Practice: Negotiate for rebates with your card issuer. Clearly this is a matter that the cardholder's organization will have to bring up; the card issuer is not going to broach the topic. As indicated above, the level of purchases needed to qualify for a rebate has been dropping.

Rebates are generally quoted in basis points, with 100 basis points equaling 1 percent. At this level, a company spending $1 million per month (or $12 million per year) might expect a rebate in the neighborhood of 5 basis points or $5,000 per month, or $60,000 on an annual basis. As programs get larger, the number of basis points the card issuer is willing to rebate grows. As with the terms, this issue can be used as a negotiating point when establishing a new program with several issuers bidding for the business.

Almost Best Practice: Ask for rebates, but don't necessarily take the first offer. If the card issuer believes the business may go elsewhere, it may become more aggressive in its offer. At a minimum, ask at least once—even if you feel your volume doesn't justify a rebate now. Let the card issuer know what you are thinking and plant the seed so that down the road, when volume increases, the issuer is ready to give your company the rebate.

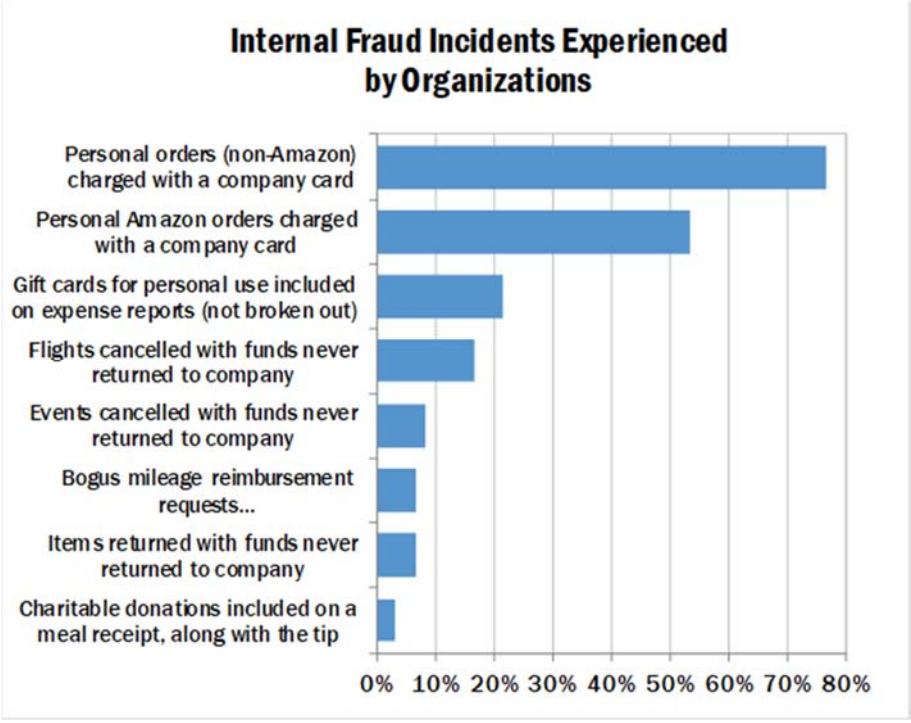
Special Pointers for Accounts Payable: This is definitely a case of "You don't ask, you don't get." In order for the company to get a rebate, it must request one—ideally during the negotiation process when the account is being set up. If you have a program in place without a rebate feature and the business is significant, broach the topic. If the card issuer is not receptive, you might suggest (with senior management's backing) that you are considering putting the program out for bid.

If your program is of sufficient size that you have one or more professionals working on it, you might want to consider membership in the National Association of Purchasing Card Professionals (NAPCP). Even if you have one person spending half their time on this issue, membership is a worthy consideration. By attending the NAPCP annual conference (or its webinars and/or regional meetings), you'll be able to keep up on the latest issues and best practices affecting your p-card program. This professional organization also runs a well-respected certification program for those who are making a career out of p-cards.

Worst Practice: Never asking for a rebate.

¶706 Employees Using Cards Deceitfully for Personal Gain

The number of ways employees defraud their employers through game-playing with cards (both company and personal) is amazing. The following chart summarizes the most common types of game-playing along with the percentage of organizations where this has been found to occur. It also provides a summary chart of best practices that will prevent and/or detect the possible frauds.



Before we take an in-depth look at the best practices, let's be clear about one thing. The percentages shown indicate the proportion of organizations that have encountered the particular item, not the frequency of occurrence. So, for example, in AP Now's Lesser-Known Fraud survey, the 76.67 percent who indicated they have found personal non-Amazon orders charged with a company card does not mean that 76.67 percent of employees will play this game, just that it happened at least once (and probably more frequently than that) at 76.67 percent of all organizations participating in the survey.

Keep in mind that the numbers shown likely understate the problem, as respondents can only report frauds they have uncovered. And, if the fraud has gone undetected, then it can't be reported. Also, if the detailed meal receipt is not required, it is very difficult to determine if a gift card was added to a bill. So, the suspicion is that this type of fraud is a bit higher than reported.

Best Practice #1: Start with a comprehensive detailed policy for both travel and use of p-card. This makes it crystal-clear what is expected. What's more, many organizations include in their p-card policy a letter. This letter must be signed by any employee who is given a company card. In the letter the employee acknowledges he or she can be fired immediately for misusing the card. This makes it impossible for employees committing the infraction to claim they didn't know. If they didn't read the policy, that is their problem, not yours.

Best Practice #2: Require managers to review expense reports as well as charges put through by subordinates on company cards. This is probably the most overlooked control in many organizations. AP Now surveys reveal that only about one-quarter of all managers regularly review the expenditures of their employees.

Most simply approve without reviewing what is on the report. This is unfortunate, because the manager is in the best position to spot potential frauds and stop them. What's more, if the manager doesn't review eventually, the employee comes to realize the manager isn't reviewing. In these instances, if so inclined, the employee will then take advantage of the situation and begin pushing the envelope.

Best Practice #3: Mandate use of the company credit card. All the tricks that involve getting refunds simply disappear if the organization mandates the use of a company card and refuses to reimburse if the employee uses a personal card. Yet, almost half of all companies (47 percent) have a travel card for employees but make its use optional. For reasons that defy logic, even best practice organizations are willing to loosen controls in this regard.

Best Practice #4: Require detailed meal receipts. Of course, requiring the receipts only works as a control if someone actually reviews them. This doesn't mean that all the receipts must be reviewed in detail, but it does mean they should be spot-checked in detail. And of course, if the manager is reviewing everything, the accounts payable staff or the expense review staff doesn't have to worry about this issue.

The fact that organizations know about gift cards and charitable contributions means that employees are putting them through. Other questionable items that our readers have shared that they found on detailed meal receipts include takeout dinners (someone bringing an extra meal home for a spouse), a case of steaks from a fancy steakhouse, kiddie meals, and more. Detailed meal receipts are also a great way to document the absence of liquor for those with grants that prohibit such reimbursements.

Special Pointers for Accounts Payable: The best practices discussed here are pretty basic, and there is no good reason why organizations neglect to use them. Probably the most difficult change for most is to get managers to review expenditures by employees. Whether they are overworked, embarrassed to be seen nitpicking over expenses, or simply believe their employees are honest, is irrelevant. They need to do a much better job in this regard, and if they do, lots of this petty game-playing will simply disappear.

Yes, many employees prefer to use their personal cards for travel so they can accumulate loyalty points. But that is beside the point. When it creates extra work and/or loosens controls, priority must be given to running an efficient operation. Use of the practices discussed here will minimize, if not eliminate, many types of petty game-playing.

Worst Practice: Thinking your employees would never play games and completely ignoring the issue.

Review Questions

27. A best practice p-card program should address all of the following issues ***except:***
    a. Who should have a card
    b. Where the card can be used
    c. Spending limits
    d. Color of the card

28. Which of the following is not a strong internal control for p-card programs?
    a. Merchant Category Code blocks
    b. Monthly review of charge card statements
    c. Unlimited dollar transactions for cardholders
    d. Strong card cancellation policies

29. Which of the following is a best practice that will increase usage of p-cards in your organization?
    a. Make use of the card optional.
    b. Only give cards to employees who request them.
    c. Don't bother educating employees on proper use of the card.
    d. Increase the number of merchants in the program.

30. When it comes to payment terms for corporate p-cards, payment is likely to be due ___ days after the receipt of the bill.
    a. 30
    b. 20
    c. 10
    d. 7

¶800 Payment Strategy

Learning Objectives

Upon completion of this chapter, you will be able to:

Create a best practice process for payments made outside accounts payable

Develop a policy that limits emergency payments

Identify ways to pay small-dollar invoices without issuing a check

As the business world gets more complex, so does the approach we take to our accounts payable function. While we still have the same problems we had years ago, we also have a whole slew of new ones. New payment approaches, mainly the shift in the United States to electronic payments, means there are some new issues to be dealt with. This is not to say that the new payment approaches should not be undertaken. To the contrary, like any other new process, they need to be implemented with the appropriate internal controls and studied early on in the game to identify any new or emerging issues. In this chapter, we take a look at best practices related to the following:

Establishing an Overall Payment Strategy
Paying Small-Dollar Invoices
A Rush or Emergency Payment Policy
Payments Made Outside Accounts Payable
Basic Fraud Protection Against ACH Fraud

¶801 Establishing an Overall Payment Strategy

Most never give a moment's thought to an overall payment strategy, unless they are considering stretching payments. But that is not what this section is about. Generally, we believe that unless there is a cash flow issue necessitating the stretching, the practice can cause more harm than good. Not only does it antagonize vendors, but it also occasionally leads to duplicate payments. And a vendor that is enraged over late payments is unlikely to return a duplicate payment.

What we want to discuss here is an overall payment strategy that every company paying bills with more than one payment vehicle (checks, p-card, ACH, wire transfer, etc.) should have. The goal is to pay each vendor in the most effective manner. Having an overall strategy is especially important to those organizations considering both an ACH program and a p-card program. It is also exceedingly important for those that want to greatly reduce the number of paper checks issued.

Some reading this may wonder why establishing a payment strategy was selected to be included in the list of best practices. As many companies are finally moving away from paper checks, it is critical that the move be done in an orchestrated, systematic way that does not create problems or issues that are not addressed. After all, the goal is a more efficient payments system, not one that is less efficient and problem-ridden.

Best Practice: Carefully evaluate each vendor and decide how you'd like to pay them, eventually. Ideally the answer won't involve a paper check. Once you've got your game plan in place, systematically convert each to the ideal payment mechanism. This may sound simple, but it will take time as no conversion goes smoothly. Start with a few vendors and once you are comfortable converting, ramp up your plan.

Almost Best Practice: Converting vendors to other payment methodologies without having an overall goal of almost eliminating paper checks.

Special Pointers for Accounts Payable: Readers without a p-card program are advised to take special care when converting away from paper. If there is any chance they will at some point in the future embrace a p-card program, be careful about converting vendors to ACH who might later be converted to p-card payments. If you convert them to ACH and they like receiving their payments in that manner, they are apt to be displeased if you switch them to p-cards. While the payment might arrive at the same time, they will

have to pay the discount fee to their bank, netting something like 97 percent of what they were receiving in the ACH environment. This does not enhance vendor relations.
Worst Practice: Having no plan or not trying to move away from paper checks.

¶802 Paying Small-Dollar Invoices

Most accounts payable departments have limited resources they can devote to the processing of invoices. It seems like there are always too many invoices for the number of processors available. This means that those large-dollar invoices that really do deserve extra scrutiny don't always get their fair share of attention because too much time is being spent just getting those small-dollar invoices processed.

But what if you could eliminate some of those small-dollar invoices? That would leave more time to thoroughly review those bigger items that deserve more attention. Since you can't just not pay low-dollar invoices, another solution is needed.
Best Practice: P-cards are an ideal solution to the low-dollar-invoice problem. By putting purchasing cards in the hands of your employees buying the small-dollar stuff that creates all the small-dollar invoices, you completely remove the problem. Now, unfortunately, not every vendor accepts credit cards so you won't completely eliminate the problem. But, through a judicious use of p-cards, you can make a serious dent in the problem, freeing up your processors to spend their time reviewing the bigger items more closely.

Of course, should you take this approach, you'll want to employ the best practices discussed in the previous chapter and institute strong controls around the process. You'll also want to make sure your payment auditors include your p-card purchases when they look for duplicate payments.
Almost Best Practice: If you can't use a p-card or the vendor in question doesn't accept them, you still may have some options. If the vendor in question sends many small-dollar invoices, consider paying from statements. This should only be done after conferring with the vendor. If this approach is taken, the system should be adjusted so invoices from this vendor cannot be entered. Typically, this works for items like office supplies, overnight shipping and hiring of temp workers. This may be the only time when it is acceptable to pay from a statement. Under virtually all other circumstances, it is considered a very bad practice.
Special Pointers for Accounts Payable: Be aware that some vendors will still send invoices even though they've been paid by credit card. They claim they can't suppress the printing of an invoice. Closely scrutinize invoices from these vendors, for they will often contain a statement saying either nothing is owed or that the invoice was paid with a credit card. Unfortunately, more than occasionally these remarks are printed in rather small font size and these invoices get paid. Identify those vendors who make it a practice of still sending an invoice and put them on an ACT (always check thoroughly) list.

Don't rely on the vendor to return these duplicate payments. Most won't. You'll either have to find them yourself or hire a third-party audit firm to identify and recover them. Either approach is costly.

Be very cautious about encouraging employees to pay for items themselves and then submit them on their expense reports. Invoices should *never* be paid through the expense reimbursement process. This is a weak control, makes it difficult to identify duplicate payments, and opens the door to fraud with those few individuals who might be tempted to divert company funds to their own pockets.
Worst Practice: Not having any strategy and paying all low-dollar invoices by paper check.

¶803 A Rush or Emergency Payment Policy

Rush checks are the bane of every accounts payable function. In an ideal world where everything operates as it is supposed to, there would be no need for rush checks, also referred to as ASAP checks. However, in the real world almost every business has those last-minute emergencies requiring an immediate payment.

The last-minute emergencies are bad enough, if they are legitimate. Unfortunately, in many organizations these last-minute emergencies are the result of a breakdown elsewhere in the organization. An invoice may have sat unapproved on an approver's desk for several weeks, a manager may have forgotten to sign up for a conference that's happening tomorrow, or a myriad of other things. When this

happens and payment must accompany the order or invoice, someone shows up in the accounts payable office asking for or demanding an off-cycle check.

This is extremely disruptive to the staff and, if it happens more than occasionally, can cause a real drop in the efficiency of the department. It creates problems for those using positive pay and may cause a duplicate payment. Finally, rush checks are more likely to be fraudulent than one produced during the normal check cycle.

Best Practice: Make it a goal to eliminate all rush checks. While you may never reach this goal, most organizations can come pretty close. Here are some techniques that will get you to that goal:

Convince management that they really are a bad idea. Use the facts discussed in this course along with some numbers demonstrating just how expensive a rush check actually is.

Make it *really* difficult for someone to get a rush check. This could include requiring a sign-off from the CFO along with an explanation of why this payment could not wait for the regular check cycle. If the CFO is a believer in eliminating rush checks, this step alone may do the trick.

Identify the causes for rush checks by keeping a log of who requests them and why. After you have a few weeks' or months' activity, you should be able to identify trends and culprits (both at your company and on the outside) and then fix the problem.

Identify duplicate payments made with a rush or manual check. Bring this to the attention of everyone involved and management. There's nothing like seeing a large-dollar amount associated with rush checks to put an end to the practice.

Insist on paying electronically instead of by check. When you do get a request for a rush check, insist on ACH payment. Hopefully, you will convince the recipient to be paid electronically in the future, eliminating them from future rush check pools.

Almost Best Practice: None. This is an issue that has no middle ground. While not as serious as saying you'll tolerate small-dollar fraud, allowing rush checks for anything but the most serious emergency opens up the door for more. It's one of those cases where if you give them an inch, they'll take a mile.

Special Pointers for Accounts Payable: This is one of those issues where you don't win any friends. Sometimes a staffer might be tempted to break the rule for a friend in another department or a popular employee. But this will come back and haunt you. As soon as others figure out what's going on, they will (a) complain and demand equal treatment or (b) have the favored employee bring all departmental requests for rush checks.

If a rush request is made without backup, follow up afterwards to get the backup. If an invoice is involved, don't forget to extinguish the purchase order and receiving documents associated with it. For if you don't and the invoice shows up in accounts payable, the odds of it being paid are quite high as there is no evidence that it has already been paid.

Worst Practice: Allowing rush checks, making no effort to minimize or eliminate them.

¶804 Payments Made Outside Accounts Payable

Research by AP Now reveals that 80 percent of ACH payments are made by the accounts payable staff. This means that 20 percent are not made in accounts payable. On the face of it, this may not seem like a big problem. But, if organizations aren't careful about this issue, they could have a huge problem on their hands.

The problem revolves around the controls used in accounts payable versus the ones used by other departments making payments. Consider the following questions.

Are they employing the same tight internal controls and strong procedures used in accounts payable?

Are they doing the three-way match?

Are they using rigid coding standards?

Are they extinguishing the PO when the transaction is complete?

Are they extinguishing the receiving document when the transaction is complete?

Are they entering the invoice number correctly?

If they aren't and a second invoice shows up in accounts payable, it will be processed correctly and payment will be made. For if the PO and receiving documents are open, why shouldn't the processor make the payment? And, it is an unfortunate reality that vendors rarely return duplicate payments without some external encouragement. This means either having someone on staff look for duplicate payments or hiring a third-party auditor. Both are expensive options for a problem that could be eliminated through some simple training and processes.

Best Practice: In an ideal world, we'd have all payments made in accounts payable to ensure uniformity in process and that proper controls and processes were used.

While this might be a recommended best practice, we want to go on record as stating we realize that if the organization is already having ACH payments made outside accounts payable, this is going to be a hard change to get approval for. We therefore expect most will have to rely on the "Almost Best Practice" approach.

Almost Best Practice: Probably a more realistic approach is to offer same training to the group making ACH payments as is given to the accounts payable staff. If you explain the reasoning in a calm and nonconfrontational manner, you are likely to get concurrence from the other department. This means you have to be somewhat of a salesperson, explaining why the fine points accounts payable insists on are so important.

Be forewarned that this will not be an easy task. Even if you get the manager of the other department to agree and the staff does attend your training, the odds are high that they will sometimes forget some of your pointers, like extinguishing an open receiver.

Pointers for Accounts Payable: More than occasionally, folks outside accounts payable don't fully grasp what can go wrong when best practices aren't followed. And, they certainly don't think about the financial implications. If your organization is one where payments are made outside accounts payable and best practices are not taken seriously, you will simply need to wait for something to go wrong. This may seem terrible on the face of it, but it's the only way to make your point, the accounts payable version of "a picture's worth a thousand words."

When you find a problem (e.g., a PO not extinguished), *nicely* point it out. Even better, if an invoice shows up and is processed and you're able to identify it as one that was paid outside accounts payable, bring this to the attention of those making that ACH payment. If you have a payment audit done (and every organization should), see if they find duplicate payments as a result of proper procedures not being followed by the group making ACH payments. Share the documentation from the audit firm to make your point.

It is imperative that if you take this approach, you do so very tactfully, avoiding pointing fingers as much as possible. Make your points as diplomatically as you can, choking back your instinct to say what's really on your mind.

Worst Practice: Do nothing and hope for the best. It will rarely turn out well.

¶805 Basic Fraud Protection Against ACH Fraud

The first thing to understand about ACH fraud is that everyone is at risk. Some think that because they do not make electronic payments, they are not at risk. Unfortunately, this is *not* true.

With the sudden onslaught of interest in ACH from both businesses and, unfortunately, crooks, a review of the basics of how ACH works is in order. For without a thorough understanding of how these payment vehicles work, it is difficult for an organization to protect itself. We cannot underestimate the importance of understanding this payment tool as both users and non-users are at risk for various types of fraud if they do not take the appropriate steps. And then, of course, there is the added benefit of ACH payments being a more efficient way to address invoices.

An ACH credit is a payer-initiated transaction. The payer instructs its financial institution to electronically transmit the payment through the ACH/Federal Reserve network to the payee's bank account. Typically, the funds are available the day after the transaction takes place. This eliminates all delays associated with mail and processing float.

An ACH debit is a payee-initiated transaction. The payee instructs the payer's financial institution to electronically transmit the payment through the ACH/Federal Reserve network to the payee's bank account. Characteristically, the funds are available the day after the transaction takes place. These transactions are initiated using your bank transit and routing number and your bank account number. It is implied that you have given your consent, but there is no formal verification process by the bank to ensure you have given your approval. There are new bank products just emerging that provide some protection against unauthorized debits.

Without a doubt, crooks have turned to the ACH to perpetrate some sophisticated frauds. These crimes are growing, and no one is immune. The crooks involved are increasingly sophisticated and the funds they steal often unrecoverable. It is important that everyone involved with payments understands the time constraints associated with identifying fraudulent ACH transactions.

As consumers, readers have 60 days to notify their financial institutions of unauthorized ACH transactions in their personal accounts. These include both ACH debits against their accounts and unauthorized ACH credits initiated from their accounts. As indicated earlier, the crooks in this arena are very smart. However, and this is a big one, anyone other than a consumer has *only* 24 hours to notify their bank of an unauthorized transaction.

There is no way around this. Monthly bank reconciliations won't cut it. Identifying a fraudulent transaction 30 days after the fact is too late.

Best Practice: There are a number of steps every organization should take to avail itself of even the most basic type of protection. Here are a few basic steps every organization should take.

Put ACH blocks on every account from which you don't want ACH activity to be initiated.

Set up a separate computer to be used for online banking and nothing else.

Institute a practice of doing daily bank reconciliations.

Put ACH filters on those accounts where you will allow limited ACH debit activity.

Educate yourself and your staff to the risk and keep updated on this issue and the products offered by banks to protect your accounts.

Realize that positive pay only protects against check fraud, not all types of payment fraud.

Almost Best Practice: None.

Special Pointers for Accounts Payable: If you identify an unauthorized transaction after the 24 hours have elapsed, don't think you have no recourse. Still notify the bank. While the bank cannot guarantee the return of all your money, it will try and recover it for you. Often the bank is successful, although sometimes it is only able to get part of the money back. Still, some is better than nothing. So, the minute you suspect an unauthorized transaction, get on the phone with your bank.

Also, if you put an ACH debit block on an account because you don't want to allow ACH debits, don't forget about it. Too often an organization puts the block on and then several years later enters into a favorable transaction that will permit a vendor to debit their account. When the first transaction hits, it is denied because of the block, leaving the vendor in a less-than-happy state of mind. Still, it is better for this to happen once than to leave yourself wide open. You can apologize and promise it won't happen again.

Worst Practice: Ignoring the issue, hoping your organization won't become a target of these insidious thieves.

Review Questions

31. Which of the following best describes a best practice approach to establishing an overall payment strategy?
    a. Evaluate your vendors and decide what payment vehicle would best meet your needs for paying each.
    b. Let vendors decide how they would like to be paid.
    c. Let the purchasing department decide how it would like each vendor to be paid.
    d. Pay everyone using paper checks.

32. Small-dollar invoices are best paid using which of the following payment vehicles?
    a. Wire transfers
    b. Paper checks
    c. P-cards
    d. Petty cash

33. Which of the following is not a best practice for minimizing rush checks?
    a. Make it difficult to get a rush check.
    b. Ask vendors if they are willing to wait for 14 days for their late payments.
    c. Insist on paying rush items electronically.
    d. Identify the root causes for rush items and work to eliminate them.

34. Payments made outside accounts payable are most likely to cause problems for which of the following reasons?
    a. The department doesn't follow the same strict standards used in accounts payable.
    b. The department only makes payments once a week.
    c. The bank doesn't recognize payments made outside accounts payable.
    d. All payments should be made in accounts payable.

35. All of the following help prevent ACH fraud, ***except***:
    a. ACH blocks
    b. Storing checks in a desk drawer
    c. ACH filters
    d. Use of a separate computer for online banking

¶900 Policy and Procedures Manual

Learning Objectives

Upon completion of this chapter, you will be able to:

Create an accurate policy and procedures manual with the least amount of fuss

Design a policy to update the policy and procedures manual on a regular basis

Because many accounts payable departments have grown gradually or evolved as part of the accounting department, few have a written game plan. Instead, procedures are developed on an as-needed basis, in kind of a hodgepodge manner. Moreover, much of the knowledge about how things work and where information is located often resides with specific individuals. If those individuals get sick or accept another job, the company is left in a lurch.

Every accounts payable department should have a procedures manual, to serve not only as a guide in case of emergency, but also to provide managers with the necessary documentation to demonstrate to management the capabilities of the staff and the work they are handling. Without such a document, few understand the scope of information that is needed to run a successful department. This is especially important for those organizations subject to the strictures of the Sarbanes-Oxley Act.

The procedures manual can also be used to determine whether any processes can be eliminated. Needless to say, this document will not be the most interesting book ever written, but it is essential. As an added benefit, it will make the auditors happy. The manual should not only be prepared by those who are actually doing the day-to-day tasks, but it should also be updated regularly. Some choose to do this anytime a process is amended or added, whereas others do it annually. It is imperative that this be done. You'd be surprised to discover just how much processes change over the course of a year.

There is one other reason to have this manual and insist that everyone follow it. Left to their own devices, processors in accounts payable will gradually develop their own procedures. Without a careful and periodic review, each person will end up handling transactions differently. There is a word for this, and it is *chaos*. If one processor has an idea for an improved way of doing a particular task, the suggestion should be raised with the manager. If it is determined that the suggestion is superior to the methodology in use, everyone should change how they handle that particular task, and the policy and procedures manual should be updated to reflect this change. In this chapter, we'll discuss:

Use of the Manual
Creating an Accounts Payable Policy and Procedures Manual
Updating an Accounts Payable Policy and Procedures Manual
Providing Access to the Accounts Payable Policy and Procedures Manual

¶901 Use of the Manual

The policy and procedures manual for any accounts payable function should be a document that is actively used in the department and in other places as well. If regularly updated and accurately reflecting processes used, it can be used in many ways. Let's see how best-practice accounts payable organizations use their policy and procedures manual.

Best Practice: A good policy and procedures manual—and by that we mean one that accurately reflects accounts payable practices in use—can be used:

As a training guide for new employees
As a reference guide for existing employees, especially for those tasks that are completed infrequently
As a reference for other departments affected by accounts payable policies.

We're not suggesting that you give everyone in the company the accounts payable policy and procedures manual. Let's be honest; few would read it. But you can cut parts of the policy into shorter one-page documents and share them with those who need it. The best example of this practice would be to reproduce

the cut-off schedule for checks. This can be given to those who submit invoices for payment so they know the schedule and know when an approved item has to be in accounts payable in order to have a check cut in the current production cycle.

Almost Best Practice: Using the manual only for some of the items listed above, not all of them. By doing this, you are not getting full value out of the efforts put into producing the policy and procedures manual.

Special Pointers for Accounts Payable: Managers who want to teach their staff to be self-reliant should point them to the manual any time they ask a question whose answer can be found in the policy and procedures manual. Sure, it's faster for them if you just tell them the correct answer, but they need to rely on the manual. This will also make the manager who spends too much time answering staff questions more productive.

Worst Practices: Worst practices include:

Not having a policy and procedures manual.

Creating a policy and procedures manual and not using it.

Creating a policy and procedures manual and not giving it to processors to use as a reference tool.

¶902 Creating an Accounts Payable Policy and Procedures Manual

An effective policy and procedures manual should contain clear, simple instructions and not much else. This is not the place for long missives on philosophy or corporate policy. This is simply a big how-to book. It is not a place to show off creative flourishes or flights of whimsy.

Best Practice: The following guidelines will help you produce a manual that can be used to run an effective and efficient accounts payable function.

Begin with a bare-bones outline listing the topics to be covered.

Use your outline to create a table of contents, breaking information into appropriate sections.

Keep your instructions short. Break longer procedures into a few short steps.

Avoid run-on sentences. Review what you've written and break long sentences into two or three shorter ones.

Use lots of bulleted and/or numbered lists (i.e., Step 1, Step 2, etc.).

Include examples wherever possible, especially when the concepts are not crystal clear.

If you include jargon or abbreviations, make sure they are spelled out. Better yet, avoid the jargon and abbreviations, if at all possible.

Include footers that number your pages.

As the next to last step, run spellcheck to find misspelled words. Be careful. As you are probably aware, spellcheck will sometimes try and change words it doesn't recognize to common words.

As your last step, go through your document and put the relevant page numbers on your table of contents.

Almost Best Practice: Acquire another organization's policy and procedures manual and update it to reflect your actual procedures.

Special Pointers for Accounts Payable: Be aware that this is a lot more work than it would seem on the face of it. Every organization handles its accounts payable function differently. So, you cannot simply take someone else's manual, make a few minor adjustments, and have a good policy and procedures manual.

Worst Practices: Worst practices include:

Having the manual written without consulting those who are doing the actual work.

Not making sure that the practices in use conform to the manual.

Allowing shortcuts that are not documented in the manual.

¶903 Updating an Accounts Payable Policy and Procedures Manual

Policy and procedures manuals have a lot in common with wills. We all know we should have one and should periodically update it, but few of us keep it updated once we *finally* get around to getting it done.

Even if you think you have policies and procedures exactly the way you like them, circumstances outside the control of the department may force a change. A move to a new accounting system, starting to use electronic payment alternatives, a demand by a key supplier, a physical move by a group within the organization, a new CFO, or any one of a thousand other things can cause the department to need to implement change.

The very best manuals are updated every time a change to the procedures is made. This is one of the benefits of posting the manual online instead of printing hard copies. Of course, this is probably not realistic in most organizations. At least once a year, the manual should be reviewed and updated. This is also a good time to ensure that the procedures detailed in the manual are actually being followed in the department. You will be surprised to find how often they are not.

Best Practice: At least once a year, and more frequently if you make a change to your processes, a review and update of the policy and procedures manual is called for. Use the following steps to complete the task:

Find your old policy and procedures manual and dust if off.

Review the manual and mark off all processes that have changed.

Make a note of new processes that need to be added.

Either assign one person to make all the changes or, better yet, assign different sections to different staff members. Ideally, the assignments should match their responsibilities.

Set a deadline when the draft material is due back. Make sure everyone is aware of the deadline.

A week before the deadline, send a reminder e-mail to everyone working on the project.

Two days before the deadline, send another reminder e-mail.

Collect all sections and review. If you disagree with anything written, discuss it with the author.

Have all changes reviewed. Do this by giving each section to someone other than the person who wrote it.

Resolve any discrepancies.

Verify that what is written in the manual is actually how the work is being processed in your department.

Publish and publicize. If at all possible, the manual should be put on your company intranet with access given to any employee who might need it. Highlight your check production and cut-off schedules.

Thank everyone who was involved.

Every six or twelve months, repeat the process.

Almost Best Practice: Updating the policy every two years.

Special Pointers for Accounts Payable: Be aware that waiting two years is really not recommended; waiting this long just makes the process all the more onerous.

Worst Practice: Never updating the policy and procedures manual.

¶904 Providing Access to the Accounts Payable Policy and Procedures Manual

Producing a policy and procedures manual for accounts payable is important. But, if once the manual is produced, it is not shared with everyone who might benefit from it, you are certainly not getting full value for your efforts. More than occasionally, the manual is given to the accounts payable manager and that's it. While there might have been some rationale for this action when we had to print documents, it no longer makes sense. PDFs cost nothing to produce, and the organization's intranet can host the manual for a minimal cost, if that. There's a lot more that can and should be done with the manual.

Best Practice: Obviously, the manager of the department should get a copy of the manual. So should every person who works in accounts payable as well as the management team that supervises accounts payable.

Finally, any procedure that involves another department should be cut out and pasted into a separate document and shared with that department. That way, they will know what is expected.

Some organizations print copies of their check cut-off schedule and then give a copy to anyone who requests a rush check, so they'll know the deadlines in the future. This can also be handled through e-mail.

Almost Best Practice: None. Providing access to everyone is important; there are no halfway steps.

Special Pointers for Accounts Payable: When sharing the manual and parts of the manual, don't forget the admins who often handle payment-related tasks for their bosses. It is probably more important that they get the information than their supervisors, as they are the ones doing the work. Don't horde the information in your manual. It should be readily shared with anyone who might have a need to see it.

Worst Practices: Worst practices include:

Limiting access to the manager and supervisors.

Not giving a copy to every processor.

Not giving copies to employees outside accounts payable who are affected by the policies and procedures laid out in the manual.

Review Questions

36. A good policy and procedures manual can be used for all of the following purposes, ***except:***
    a. As a training guide for new employees
    b. As a reference guide for the accounts payable staff
    c. As a reference guide for others in the company
    d. As a training guide for sales

37. Which of the following should be used in a best practice policy and procedures manual?
    a. Long descriptive paragraphs
    b. Bulleted lists
    c. Links to descriptions elsewhere on the Internet
    d. An explanation of the organization's personnel policies

38. What is the recommended best practice for updating the policy and procedures manual?
    a. Never updating it
    b. Updating it every two years
    c. Updating it every time a change is made
    d. Updating it every five years

39. Who should have access to the policy and procedures manual?
    a. Only the accounts payable manager
    b. Only the invoice processors
    c. Only upper management
    d. Anyone who might need to reference it

¶1000 Operational Aspects

Learning Objectives

Upon completion of this chapter, you will be able to:

Create a strategy to avoid double payments when the original invoice is missing

Develop a policy to limit the intrusions in accounts payable

Identify lost funds through an effective supplier statement review policy

There are a number of tasks that accounts payable has to take on that do little or nothing to adding value but still must be done. In this chapter, we take a look at a few of those tasks that relate to the operational aspects of accounts payable. They are:

Paying When the Original Invoice Is Missing
Limiting Calls to Accounts Payable
Petty Cash
Reviewing Supplier Statements
Adopting a Policy of Never Returning Checks to Requisitioners

¶1001 Paying When the Original Invoice Is Missing

Inevitably, no matter how good your processes are, an invoice will not arrive in accounts payable for payment. It may be lost in the postal mail, lost on an approver's desk, or lost in intercompany mail. Getting a replacement to process and pay can be tricky, if you don't want to make duplicate payments. And, we're going to go out on a limb here, and assume that since you are taking this course, you don't wish to make duplicate payments.

It used to be considered a best practice to never pay from a copy. That's when it was relatively easy to identify a copy just by looking at it. It was before the use of PDFs and electronic invoicing became commonplace. Today, with a PDF copy of an invoice, you can have 100 copies of the same invoice and each one looks just as good as the next, making it impossible to determine which is the original and which is the copy. Hence this practice no longer works. Truth be told, this has become less of an issue because it is so difficult to tell a copy from the original. So often, a second invoice is simply submitted and no one realizes it isn't the original.

Unfortunately, when a copy or second invoice is sent, very few vendors actually mark the document as "COPY" or "Second Invoice." Thus, it is imperative that the staff be able to use other tactics to identify a duplicate invoice. But occasionally an invoice is truly lost and a copy is needed.

Best Practice: Assuming that you realize the invoice being submitted is a copy or a duplicate, take the following steps;

Go through the normal three-way match.
If that works, check the vendor's account to make sure no payments were made for the exact same amount.
If payment is being made on a check request form, go through the three-way match and make sure the PO and receiving document are extinguished.

Almost Best Practice: None.

Special Pointers for Accounts Payable: As we move into an age where an increasing number of invoices are e-mailed or delivered electronically, this will be less of an issue. However, what will become a bigger issue is the matter of identifying duplicate invoices that should not be paid.

This also means that whenever an invoice shows up in accounts payable for payment greatly past the due date, it is incumbent on the staff that some extra checking be done to verify that this invoice has not

already been paid. It could have been processed as a rush payment, in which case normal best practices may not have been followed.
Worst Practice: Making no special arrangements to pay when the original invoice is lost.

¶1002 Limiting Calls to Accounts Payable

Very few tasks waste more time and add less value than responding to vendor inquiries. Sometimes the vendors themselves call; other times, the purchasing professional who works with them calls. Yet, inquiries must be handled and addressed in a timely manner. The issue is how to address this need without using valuable resources that could be diverted to more value-add tasks.
Best Practice: The best way to address this issue is to make available an online payment status portal giving vendors the opportunity to check their payment status online, whenever they want. In the very best online portals, they can check:

Date payment was made
Date payment is scheduled to be made
If invoice has been received

In an ideal situation, in these portals or as part of an e-invoicing system, an online dispute resolution module is included. This allows both sides of the transaction to communicate without ever having to pick up the phone. It also provides an electronic audit trail, so if one party is failing to communicate, it is readily apparent to anyone who checks.
Almost Best Practice: Assuming that an electronic solution is not available, try one or more of the following to get a handle on the onslaught of calls.

Set a particular time when calls will be accepted, say Tuesdays and Thursdays between 1 p.m. and 4 p.m.
Assign one person to handle all calls.
Respond to all inquiries within 24 to 48 hours.

Special Pointers for Accounts Payable: One of the ways to avoid the calls is to anticipate calls and provide information so the call does not have to be made. This is especially true when it comes to providing data about deductions. Often, calls are from accounts receivable staff trying to apply cash. By making sure deduction information is sent along at the time of the payment, many of the calls can be avoided.

Some organizations choose to have each processor handle vendor calls related to the accounts they handle. The rationale for this decision is that they know the accounts best. And this is an important factor to take into consideration. However, if they are constantly interrupted with calls, their productivity will diminish. What's more, each person has their own set of skills. Handling disgruntled vendors is not something everyone is adept at. Better to hire one or two people skilled in dealing with difficult situations to handle the vendor calls and let the staff focus on what it does best: processing invoices.

Additionally, if payment is made on time, the "where's-my-money" calls diminish in number greatly. While payment timing is usually not decided in accounts payable but at a higher level, the additional calls and how to address them should be taken into account when considering stretching vendor payments beyond the previously agreed to terms.
Worst Practices: Worst practices include:

Not addressing the issue.
Not responding to inquiries in a timely manner, necessitating a second call.

¶1003 Petty Cash

Petty cash boxes have been with us for ages. The intent was to reimburse employees quickly for out-of-pocket expenses that could not be put through on expense reimbursement requests. The potential abuses of petty cash are huge. What's more, even where no malfeasance is intended, petty cash boxes are frequently out of balance, and rarely is there more money in the box than expected.

Petty cash boxes made sense when credit cards weren't common and corporate credits were not used by most organizations. That ship has sailed. There is really no good reason today to have petty cash boxes. Yet, anecdotal evidence suggests that about 25 percent of all companies still have them. For many, it is a corporate culture issue.

Best Practice: Completely eliminate the petty cash box.

Almost Best Practice: Work to reduce the number of items and dollar level of items reimbursed through petty cash.

Special Pointers for Accounts Payable: If you glance below, you will notice that there are many more worst practices associated with petty cash than there are best and almost best practices. This is a sign of the problems the petty cash box can cause.

If there is a petty cash box, surprise audits should be part of the routine. What's more, like the master vendor file, access to the box should be severely limited. For if it isn't and there's a problem, there will be a lot of finger-pointing and no way to determine who really is responsible for any losses. It goes without saying that all transactions should be approved, reviewed, and recorded in a log and the box should always be in balance.

Worst Practice: Worst petty cash box practices include:

Allowing unlimited reimbursements in the petty cash box.

Not prohibiting reimbursing for items that should have been put through on an expense report.

Reimbursing for items that are expressly prohibited in the corporate travel policy.

Cashing personal checks in the petty cash box.

Accepting IOUs in the petty cash box.

Not limiting the number of people who can go into the box.

Not keeping the petty cash box locked and out of sight in a secure location.

Not establishing a set time each week to handle reimbursements.

¶1004 Reviewing Supplier Statements

Some suppliers send statements because they want you to check them for any invoices you may not have received. Most accounts payable departments don't have the time to do that, although a few do. But there is a good reason to look at these statements, and that is to find any open credits you may have but don't know about. The vendor may have sent a credit memo to purchasing or may not have sent it at all. When the credit memo gets to purchasing, it is often filed or thrown away if the purchasing manager doesn't know what to do with it. Of course, many vendors never send credit memos, so unless you take action, there's no way you'd know about them or use them.

There is one other dirty little corporate secret regarding vendor credit and supplier statements. Some vendors intentionally suppress open credits when they print statements to send to their customers. If you think this isn't true, ask yourself this: Does your accounting system have the ability to suppress credits when printing statements? Many do, and that functionality is in there for only one reason: end-users wanted it.

If you are wondering what happens to credits vendors never reveal to their customers, you're in for another surprise. In the past, sneaky vendors used to write off those credits to miscellaneous income. Unfortunately for them, when the state unclaimed property auditors show up, one of the first things they ask for is the miscellaneous income account and backup for all items. Open vendor credits are considered abandoned property by most states and, as such, should be turned over to the state as part of the unclaimed property reporting.

Vendors who have no wish to do that have found another use for these open credits. They apply them to unearned early payment discounts, late fees (that you refuse to pay), and disputed items that you had no intention of paying. While some vendors who do this have good intentions and believe they are doing you a favor, others know exactly what they are doing.

Best Practice: Request vendor statements from all vendors at least quarterly. When the request is made, make sure the vendor understands you want statements showing all activity, not just outstanding invoices.

Once you get those statements, review them closely and recover all open credits. You can do that by either applying the credits against new invoices or requesting the vendor cut you a check.

Some vendors will dig in their heels insisting you place a new order if you want the credits. Don't fall for that trick. It's your money and you are entitled to it.

Almost Best Practice: None. This is money that comes right off your organization's bottom line. There is no halfway approach to this problem.

Special Pointers for Accounts Payable: Not everyone has the resources to continually check vendor statements. If you don't, hire an outside third party to do this for you. It should be noted that this is where most duplicate payment audit firms begin their recovery efforts, as these recoveries are viewed as low-hanging fruit. There's no reason to pay someone to get the easy stuff. Do it yourself and then call in the pros to find the more difficult duplicate and erroneous payments.

Worst Practice: Ignoring the vendor credit issue completely.

¶1005 Adopting a Policy of Never Returning Checks to Requisitioners

Returning checks to requisitioners is a royal nightmare for accounts payable. First, it introduces exception processing into the function. Someone has to identify the check that needs to be returned and then it has to be pulled from normal processing. And that is only the beginning of the disruption. Then a call or e-mail must be sent to the person requesting the return of the check to come and pick it up, or it must be delivered. Sometimes an admin comes to get the item, and other times the person making the request picks it up.

This is where the real fun starts. The check doesn't always get delivered. Sometimes it languishes on the exec's desk, eventually getting buried under papers. Other times, the meeting at which the check was to be delivered is canceled and the check forgotten.

It doesn't really matter what the scenario, if the check isn't delivered, eventually the vendor will start looking for its money and call accounts payable. Again, this requires more accounts payable resources to deal with the situation. None of these tasks adds any real value to the process.

And, we haven't even begun to address the fact that a few unscrupulous employees know that if they get their hands on a check, they can probably cash it and pocket the money themselves. And, that is precisely what a few employees do. In one well-publicized case, an event planner for a well-known company used this approach to rip off her company for more than $1 million over the course of several years.

Best Practice: Never return checks to requisitioners. This should be your company policy.

Almost Best Practice: If you can't enact a never-return-a-check-to-the-requisitioner policy, there are additional steps you can take to make sure that only a very few checks are returned and only under extreme circumstances. Develop a form that must accompany each request that the check must be returned. It should include:

An explanation of why the check must be retuned, and

The signature of a senior-level executive.

If the senior-level executive is sympathetic to the plight of accounts payable and agrees that returning checks is not a good idea, requiring his or her signature is likely to dissuade all but the most diehards. And having to explain in writing why the check must be returned will deter those with marginally acceptable excuses.

Special Pointers for Accounts Payable: This is an issue that has faded somewhat. In the past, the real excuse, although it was seldom voiced, was that the person requesting the return of the check wanted it returned so he or she would be asked out to lunch by the supplier accepting the check. This seems to be less the case in current times.

Often, requests that checks be returned to the person putting them in for payment are also rush or ASAP checks. This is a double whammy and double cause for concern. If, as previously recommended, the rush payment is made electronically, the return issue disappears. If not, special care should be taken, including the form with the reason and the executive signature.

Worst Practice: Returning checks to anyone who asks.

Review Questions

40. Which of the follow is ***not*** a reason why it is difficult to identify duplicate invoices?
    a. They are rarely identified as duplicate or copy.
    b. They are sent on different colored paper.
    c. Duplicate invoices look just like original invoices.
    d. You can print 100 copies of a PDF invoice and they all look like originals.

41. What is the best practice way to reduce/eliminate calls to the accounts payable department when looking for payment status?
    a. Refuse to accept such calls.
    b. Direct such calls to purchasing.
    c. Set up a vendor portal with this information.
    d. Pay all invoices as soon as you receive them.

42. What is the best practice associated with petty cash?
    a. Limit the items that can be paid through petty cash.
    b. Eliminate petty cash completely.
    c. Allow employees to submit for petty cash reimbursements anything under $100.
    d. Reimburse though petty cash any time of the day.

43. From a best practice standpoint, how often should vendor statements be requested and reviewed?
    a. Never
    b. Annually
    c. Quarterly
    d. Monthly

¶1100 Duplicate Payment Issues

Learning Objectives

Upon completion of this chapter, you will be able to:

Design processing standards to limit problems

Develop routines to avoid making duplicate payments

Craft an effective policy for requiring backup for rush payments

It's a sad fact of corporate life, but many organizations regularly pay a very small percentage of their invoices more than once. An unfortunate part of the duplicate payment issue is the large number of companies that truly believe they never make a duplicate payment. While their processes may be first-class, mistakes happen. Additionally, fraud happens and the crooks who perpetrate invoice fraud know about duplicate payment checks—and they also know how to circumvent them.

In this chapter, we'll discuss:
Using Processing Standards
Duplicate Payment Avoidance
Mandating a Rigid Work Process or Eliminating Creativity When Processing Invoices
Some Quick Checks to Identify Duplicate Payments
Backup for Rush Checks

¶1101 Using Processing Standards

While most in accounts payable would like to believe that others are the cause for their mistakes, the reality is that sometimes mistakes are made in accounts payable, especially when each processor handles invoices in the manner he or she believes is best. It's not that what one person is doing is wrong; it's just that unless everyone processes invoices in exactly the same manner, there are going to be duplicate payments introduced.

Best Practice: To ensure a best-practice accounts payable function:

Establish detailed practices that each processor must use.
Develop a rigid coding standard to be used when entering data.
Periodically check your processors to make sure they are using the prescribed routines and not shortcuts they've developed on their own.

The coding standard should cover every possible permutation of data entry. Here are a few issues to be addressed:

The way individual's names are entered (first name first or last name first)
The way abbreviations are handled (IBM or I.B.M. or I B M)
How to handle leading modifiers (The Gap or Gap)
Use of full names or abbreviations (IBM or International Business Machine)

Don't forget to address industry-specific issues, how to enter postal addresses, titles, and how to enter invoice numbers (whether to include spaces, dashes, leading zeros, etc.).

Almost Best Practice: There are no almost best practices. You either do this and are successful or you don't—in which case, you'd better be using a payment audit firm.

Special Pointers for Accounts Payable: If you take this step seriously and really set up rigid processes and rigid coding standards, you will almost completely eliminate duplicate payments. It may seem like I'm harping on this issue. It's for a very good reason. This stuff pays off.

Worst Practice: Not establishing rigid processes and data entry coding conventions for the staff to use when processing invoices.

¶1102 Duplicate Payment Avoidance

The best protection against duplicate payments is to make sure they don't happen in the first place. Now, if you're thinking, "Duh, we know that," realize that not making them in the first place is not as easy as it sounds. What's more, some executives firmly believe their organization never makes a duplicate payment and alas, they are rarely correct. It's like the people who say they never make a mistake.

Best Practice: Best practices that help prevent duplicate payments in the first place include:

Use of best practices and strong internal controls around the master vendor file

Timely payment of the original invoice

Use of rigid coding standards for data entry when processing invoices

Reducing or eliminating all rush checks

Regularly cleansing the master vendor file of inactive and duplicate vendors

Each time a duplicate payment is identified, reviewing the paperwork to see if you can identify the root cause. Once that cause has been identified, work to eliminate the problem.

Almost Best Practice: None; nipping the duplicate payment issue revolves largely on the use of rigid coding standards.

Special Pointers for Accounts Payable: Duplicate payments will happen, regardless of how tight the controls are. Accounts payable is often concerned that they will be unfairly blamed for any duplicate payments. Occasionally that happens. More often, it provides accounts payable with the ammunition needed to get the changes they want implemented. Too often, accounts payable staff know that processes should be changed or improved, but they cannot get the resources or support needed to implement those changes.

There is another untold tale related to duplicate payment audit firms. Some of them report that they go back to the same companies year after year, finding the same type of duplicate payments over and over again. It's not that the audit firm hasn't given recommendations for change—the company has just not implemented them.

Insist that the duplicate payment audit firm not only recover funds, but also identify procedural weak spots in your organization. The firm should also make recommendations as to what the company can do to tighten its policies and procedures. The recommendations from the audit firm are often the turning point that gets management moving.

Worst Practices: When it comes to preventing duplicate payments, some organizations are back in the dark ages. Worst practices include:

Relying on the "memory" of the accounts payable associate to identify duplicate payments. This is an atrocious practice that is unfair to the accounts payable associate, but is still used at some companies.

Having no duplicate payment checks in your process.

Not implementing any of the recommendations made by the duplicate payment audit firm.

Not using an outside audit firm to check for duplicate payments.

¶1103 Mandating a Rigid Work Process or Eliminating Creativity When Processing Invoices

Standardization in the process is the key to avoiding payment problems in the accounts payable function. Without rigid standardization, a second invoice will be processed and paid should it show up in accounts payable. This necessitates the tedious and expensive task of identifying and recovering duplicate payments.

Managers who require their staff to rigidly adhere to a standardized process are occasionally accused of being control freaks. This is unfortunate, for all they are doing is the best job possible at protecting their organization's assets. When it comes to processing invoices and other related tasks, creativity is to be actively discouraged. As we'll discuss, there is a way to incorporate new and better processes. It just has to be done in an organized manner.

Best Practice: Develop detailed standardized instructions for how an invoice is to be processed and how data is to be entered. This must include a rigid coding standard. These instructions and coding standards should be included in the accounts payable policy and procedures manual.

All processors should be trained using these standards. They should also be given their own copy of the accounts payable policy and procedures manual. Since it is frequently in the form of a PDF file, distributing copies isn't difficult or expensive.

Periodically check each processor's work to ensure he or she is using the approved standardized instructions.

Should a processor have a suggestion on how the workflow could be improved, he or she should be encouraged to share this with the manager. The manager can then evaluate the suggestion, making sure that besides making the task at hand more efficient, it won't introduce any internal control weaknesses.

After the manager is certain that the suggestion will improve the accounts payable process without introducing internal control weaknesses into the system, an evaluation needs to be made of how the suggested change would impact other departments affected by the change. If they will be impacted, a discussion with them is called for to decide if they can work around the change or if it will cause them real problems.

Once everyone is in agreement that the recommended change is a good thing, it can be introduced to everyone handling the task in question. Everyone affected should be trained and begin using it on the agreed-upon date. Lastly, the accounts payable policy and procedures manual should be updated to reflect the change.

Almost Best Practice: None; this is another one of those all-or-nothing practices.

Special Pointers for Accounts Payable: By sticking to the rigid standardized procedures and using the mandated coding standard, most organizations are able to eliminate close to 100 percent of all duplicate payments. But this only works if everyone sticks to it, allowing no exceptions.

Worst Practices: Worst practices include:

Allowing processors to each handle their task as they think best.

Not having detailed standardized procedures for all to follow.

Not fully considering new recommendations.

Allowing processors to develop their own workarounds or shortcuts.

¶1104 Some Quick Checks to Identify Duplicate Payments

Most organizations recognize that even with the most stringent controls and use of best practices, duplicate payments occasionally slip through. This can occur when:

Invoices get lost in the mail.

Invoices sit on an approver's desk for weeks.

Companies decide to stretch terms and the supplier sends a second invoice because it did not get paid.

Rush or manual checks are used.

Fraud is committed, by vendors and employees.

Disputes are not resolved in a timely manner.

A myriad of other factors.

Therefore, it is critical that they do some checking to ensure this doesn't happen.

Best Practice: As discussed above, use of standardized processes and rigid coding standards will help eliminate duplicate payments. Additionally,

Identify the dollar level of what your organization considers a big invoice, say $100,000 or perhaps $25,000, and double-check these larger payments to ensure that a duplicate payment is not being made.

Create an ACT (always check thoroughly) list for vendors who tend to have duplicate payments more frequently than others. Routinely double-check all transactions with that vendor. Similarly, if certain approvers tend to be associated with more duplicate payments, work with that approver.

Review payments for identical payment amounts paid to different vendors.

Using a payment audit firm to identify and recover duplicate and erroneous payments.

Almost Best Practice: Any other routine you can create that checks to make sure you haven't already paid the invoice in question.
Special Pointers for Accounts Payable: The companies that believe they do not ever make duplicate payments are often reluctant to bring in a duplicate payment audit firm. Since most of the duplicate payment audit firms work on an incentive basis, earning a percentage of what they find, bringing one in costs nothing. The other reason some companies object to duplicate payment audit firms is they think they are too expensive. With an audit firm, as previously noted, at least the company collects a percentage of the duplicate payment—without it, the company collects nothing. The real response to that claim is that it is more expensive not to use a payment audit firm.
Worst Practice: Doing nothing to identify and recover duplicate payments.

¶1105 Backup for Rush Checks

Rush checks, also referred to as *emergency checks* or *ASAP checks*, create headaches for accounts payable departments. They are those checks produced outside the normal check production cycle. They are supposed to be for once-in-a-lifetime emergencies that crop up with varying frequency depending on the nature of the business and the tolerance of the corporation for this type of behavior.

In reality, they are sometimes written to cover for the sloppy habits of certain employees. These may be executives who get behind in their work and neglect to approve invoices for payment, harried purchasing managers who lose an invoice in the stacks of paper on their desk, or the late-to-the-game employee who rushes in an expense report the day her credit card bill is due.

The problem with these transactions is that an employee in the accounts payable department is forced to stop his work to process the rush request. What's more, payment audit firms report that there is an increased risk for a duplicate payment any time a check is written outside the normal cycle. The cost of recovering duplicate payments is huge.

There is one other consideration when it comes to rush checks: the increased risk of check fraud—especially if the checks are also returned to the requisitioner. Finally, let's not forget that often the check issuance files given to the bank for positive pay are sloppily updated. This means more calls from the bank on this issue.

These problems are compounded by the fact that often the backup associated with rush checks is slim to non-existent.
Best Practice: Insist on full documentation for every rush request. This will enable the accounts payable staff to run the item through the standardized processes, including the three-way match. If the backup is missing, make the payment if you must, and then attempt to get it in the next few days. If you don't and the original invoice shows up, payment will in all likelihood be made.
Almost Best Practice: The harsh reality is that few companies can afford to take such a harsh stance. Nor are all senior management teams willing to back such a practice. Few accounts payable associates are willing to tell the secretary of the president of the company that a check will not be issued for the president, regardless of the reason. A more reasoned approach is to issue rush checks without backup occasionally under very strict guidelines.
Special Pointers for Accounts Payable: While the accounts payable department is well aware of the problems associated with rush checks, accounts payable managers also need to be aware of the corporate culture within their own organization. If the purchasing manager asks for a rush check and accounts payable refuses, he is likely to go over their heads. It is imperative that accounts payable has a good read on how management will react. If 95 times out of 100, it will back the purchasing manager, then accounts payable managers are advised to avoid the confrontation, grit their teeth, and find ways to work with purchasing to reduce the number of these incidents.
Worst Practice: Unfortunately, when it comes to rush or emergency payments, many terrible practices are being used today. They include, but are not limited to:

Issuing manual checks whenever anyone asks.

Requiring little or no documentation proving that the rush request has not already been honored.

Not checking for duplicate payments.

Review Questions

44. Which of the following is ***not*** part of a best practice accounts payable processing function?
    a. Sharing the organization's personnel policy with all processors
    b. Establishing detailed practices for all to use
    c. Developing a rigid coding standard for data entry
    d. Periodically checking to verify processors are using standards established

45. Which of the following practices will help prevent making a duplicate payment?
    a. Weak master vendor file controls
    b. Timely payment of original invoices
    c. Strict vacation policy
    d. Mandatory overtime at year end

46. How should a best practice accounts payable operation direct its processors to handle invoices?
    a. Be as creative as they like.
    b. Follow rigid standards set by the manager and used by others in the department.
    c. Use the standards they used at their prior company, especially if that organization was known for its best practices.
    d. Do whatever they like.

47. Which of the following is not a recommended practice to stop duplicate payments?
    a. Double-checking payments on high-dollar invoices
    b. Double-checking payments to vendors known to submit duplicate invoices
    c. Reviewing payments looking for identical dollar amounts
    d. Reviewing payments looking for early payment discounts

48. Which of the following is a worst practice when it comes to rush checks?
    a. Limiting the number of rush checks
    b. Issuing a rush check to anyone who requests one
    c. Making rush payments with ACH instead of paper checks
    d. Requiring an approval from a senior-level executive to issue a rush payment

¶1200 Internal Controls

Learning Objectives

Upon completion of this chapter, you will be able to:

Understand the importance of segregation of duties

Integrate the concept of segregation of duties across the payment process

Develop a list of issues to address when an employee leaves the organization

Uncover practices that will eliminate weak control points

The backbone of any well-run accounts payable function is the incorporation of strong internal controls. Luckily, a good internal control structure goes hand-in-hand with best practices, so there is never any debate on that front. Without good internal controls, mistakes are more likely to occur and the door for an unscrupulous employee, vendor, or outright crook is opened just a little bit wider. In this chapter, we'll investigate the following issues:

Appropriate Segregation of Duties
Appropriate System Access
Policy When Employees Leave
Eliminating Weak Control Practices
Staff Training

¶1201 Appropriate Segregation of Duties

Whenever the topic of internal controls is raised, inevitably the issue of appropriate segregation of duties is raised. It is sometimes called *separation of duties*. In government, the related concept is that of checks and balances. It is the theory of having several people completing a task with no one person responsible for the entire operation.

When we talk about segregation of duties in accounts payable, we actually extend the concept to the entire procure-to-pay function (P2P). The idea is that no person can handle more than one leg in the P2P process. This makes collusion necessary to perpetrate certain frauds, thereby making it harder for those few employees trying to play games and get money they are not entitled to.

Best Practice: The entire P2P function is analyzed, and no employee has the ability to perform more than one leg of the transaction. Additionally, certain tasks provide the potential for collusion and should not be performed by the same person. For example, the employee who handles bank reconciliations should not also be responsible for unclaimed property.

Almost Best Practice: There are no almost best practices.

Special Pointers for Accounts Payable: Alas, this can be problematic in smaller departments as there are not enough employees to adequately incorporate a full segregation of duties. Under these circumstances there are two options as follows:

1. Most typically, certain tasks have to go elsewhere; or
2. Additional checks are built into the process to ensure there's no fraud.

The most common task that ends up leaving accounts payable is responsibility for the master vendor file. If the purchasing staff isn't sufficiently large enough either, the master vendor file sometimes ends up in another area in accounting. While it's nice to have it in accounts payable, that is not the critical issue.

What is key is that it is handled in a unit that can:

Provide the appropriate segregation of duties and

Will take the task seriously and handle it in a timely manner.

The other task that sometimes gets moved out of accounts payable is that thankless job of getting manual signature put on checks, if that is required. This is a task that most accounts payable departments are only too happy to have someone else take on.

Unclaimed property reporting, check printing, and issuance of Form 1099s are other tasks that also get moved, if needed.

Regrettably, as long as everyone isn't 100 percent honest in the workplace, segregation of duties will be an issue all are forced to deal with on a regular basis. This could become a challenge as companies automate their accounts payable function, start making electronic payments in serious numbers, and continue to implement process improvements that make the entire accounts payable function more efficient. These very positive actions will result in smaller, more proficient staffs.

Worst Practice: Ignoring the segregation of duties issue completely.

¶1202 Appropriate System Access

This is an internal control issue that falls across all departments. But this work is only focused on accounts payable, so that's where we'll direct our attention. Most organizations are pretty good about setting up each employee with the correct system access when they first are hired. But that's where many organizations stop. After that, they do a lousy job of handling appropriate system access. They neglect to make any changes when a person is promoted or takes another position either inside or outside the company.

Consider the following, admittedly contrived, scenario. As you will be able to tell, it is constructed to make a point. Let's say you hire a new associate to process invoices. The person is given limited system access so all she can do is process invoices. This is how it should be. After some time, an opening arises and you need someone to handle the printing of checks. The processor in question has done a good job for you, so you promote her—and, of course, give her system access needed to handle the printing of checks. After a year or two, you have another opening. This time it's to handle the master vendor file. Again, the processor is promoted and given access to add new vendors or change information about existing vendors.

Can you see the problem? If each time the person in the example was promoted, the old system access was not cut off, you could have a real internal control issue. You'd have someone who could set up a new vendor in the master vendor file, enter and process invoices, and print checks to pay the invoice. This would be a real breakdown in your internal controls.

Best Practice: The answer to this issue is to simply cut system access whenever someone leaves a position. This should be done regardless of whether they've left the organization or simply taken on different responsibilities, as in the example above. Often, this issue is not addressed in a timely manner, and when it finally is after many years, the organization is horrified at what it finds. Hopefully, the organization doesn't discover this problem because an unscrupulous employee took advantage.

Almost Best Practice: Periodically run a report showing the system access for every single employee. Often, despite our best intentions, access isn't terminated when it should be.

Special Pointers for Accounts Payable: This task is often neglected when someone leaves the organization. The thinking is, "what harm could they possibly do?" The answer to that retort is "quite a bit." Just because an employee left under favorable circumstances doesn't mean that he or she isn't quietly harboring some resentment towards the organization. Don't take any chances. Terminate their access.

You know you have the problem if you ask someone who works for you to pull up information you should be getting from another department. This will happen when you've hired someone internally from another group. If he or she can get into other department's records, one of your former employees can probably access the accounts payable information.

Worst Practice: Not addressing this issue and not taking it seriously.

¶1203 Policy When Employees Leave

When an employee leaves the company, he or she still has access to a number of things, unless steps are taken to cut those ties. Among other things, these can include:

Access to the building, if the key and/or employee identification card have not been returned

Access to the computer system, if it has not been terminated as discussed above

Access to credit card sales, if the credit card has not been returned and canceled with the bank

Access to potential expense reimbursement requests, if the employee has not been inactivated in the master vendor file

Access to e-mail, unless the account has been blocked or all messages automatically forwarded to a current employee

The ability to sign a check, release a wire transfer, or initiate or release an ACH payment on behalf of the organization

Best Practice: Whether HR's plate is already overflowing or not, they are the central repository for information about all employees. They are also typically involved with all employee separations, whether pleasant or remarkably unpleasant. This means that they are in the best position to notify everyone who needs to know about an employee departure.

As it relates to accounts payable, this means some departing employees have the access to do real financial harm to the organization, unless appropriate and timely action is taken. Therefore, it is critical that accounts payable be notified so they can inform the bank and terminate the financial privileges of the departing employee.

By notifying IT at the same time, the accounts payable function is protected, assuming IT cuts the associated system access.

Almost Best Practice: When HR doesn't notify accounts payable, some steps can be taken to work around the issue. Some best practice organizations, concerned about tight internal controls, perform some of these tasks in addition to the best practices discussed above to ensure they are well protected. The additional procedures include:

Periodically getting a list of inactive cardholders from the financial institution issuing the cards and investigating whether those on the list have left the organization or are simply not using their cards

Periodically getting a list of active employees and running it against the list of cardholders and authorized signers to identify employees who have left

Periodically running a report showing which employees have access to accounts payable functionalities and closing those that should not be in place

Special Pointers for Accounts Payable: Occasionally, management will be lulled into a false sense of security, thinking that a departing employee was happy with the company and thus not taking proper steps. Don't fall into that trap. Don't underestimate the importance of taking care of what some think of as loose ends. They are anything but that.

Worst Practice: Not making arrangements to eliminate access when an employee has left the organization.

¶1204 Eliminating Weak Control Practices

Most organizations have a few weak control practices that can cause trouble. For many, these practices have been around for years and no one has taken the time to identify and end them. In some cases, this is because doing so will make management unpopular and in others, it's simply a matter of inertia.

Best Practice: Identify practices that introduce potential control weaknesses into your process and systematically eliminate them. These might include several of the previously discussed issues below:

Petty cash box

Returning checks to the person who requested them

Allowing more than the occasional true-emergency rush check

Not enforcing the T&E policy equitably across the board

Not using positive pay
Not having a payment audit
Not mandating the use of a corporate T&E card
Not cutting off systems access when an employee leaves a position

You can probably identify many more. From time to time, you'll identify practices that do not provide the tight controls you want. Or you'll find weaknesses in your existing process, perhaps due to some other change. As soon as you find these items, work to eliminate the weaknesses and strengthen your controls.
Almost Best Practice: None.
Special Pointers for Accounts Payable: Accounts payable is in a state of flux, and we expect that to continue for the foreseeable future. As new technology rolls into the workplace, practices will change. As those changes are introduced, it is critical to ensure that along with the productivity savings afforded by the new technology, you do not allow weakened internal controls to find their way in as well.

This means that whenever a process is changed, special attention is paid to the internal control aspects of the revised procedures. Expect to find weaknesses from time to time. This will require additional changes as you make sure the weakened controls are eliminated.
Worst Practice: Allowing practices that you know are weak to continue without looking for ways to eliminate them and/or tighten controls around them.

¶1205 Staff Training

Continuing professional education and staff training took a serious hit when the economy turned down. To be fair, it probably would not be right for a company to lay off a portion of its workforce while spending limited resources for others to attend seminars and/or conferences. But keeping up is more important than ever. Regulatory requirements are increasing, regulatory compliance is being scrutinized more than ever before, technology is making inroads and across the board, best practices are changing.

This means that in order to be effective, some resources will have to be devoted to professional development. In the past, this expense was largely shouldered by the organization. In many cases, it still is. As the economy begins to turn around, those organizations that cut their training budgets to the bone or eliminated them entirely are being urged to put those funds back in the budget.
Best Practice: Make sure your employees have access to the latest information about all matters related to accounts payable, including but not limited to:
Best practices in accounts payable
New technology
New frauds and tactics to thwart those frauds
Latest regulatory requirements (Form 1099, unclaimed property, sales and use tax, etc.)
Customer/vendor relations
IRS regulations related to expense reimbursements
New regulations like the proposed corporate reporting (repealed before effective date) or Sarbanes-Oxley requirements (now effective)

This can be done by allocating budget for conferences, seminars, or webinars. But, some of the technology requirements can be handled by attending some of the free vendor webinars. Professional associations, such as the Institute of Financial Operations, and fee-based newsletters, such as *Accounts Payable Now & Tomorrow*, also offer great information. And of course, there are a number of current books on accounts payable and accounts payable related topics.
Almost Best Practice: None. If the organization doesn't make a commitment to keeping its employees educated, the responsibility will fall to the employee. If that happens, some will rise to the occasion, but others won't.
Special Pointers for Accounts Payable: While it is recommended that staff training on generic accounts payable issues, such as those listed above, be obtained from outside sources, training about the organization's actual policy and procedures must be done in-house.

As suggested elsewhere, the accounts payable policy and procedures manual, if kept updated, is an excellent tool for educating new staff. Instructing of new staff isn't the only training that should go on in accounts payable. Any new process or change in procedures should also include training for everyone. And finally, periodically, the manager should review the work as the staff is performing it to see if any re-training might be required.

Worst Practice: Ignoring the staff training issue completely.

Review Questions

49. Which of the following appropriately describes the concept of segregation of duties with respect to the accounts payable function?
    a. No one person can handle more than one leg of the procure-to-pay function.
    b. No one in accounts payable can help out in personnel.
    c. The computer system for accounts payable must be separate from the computer system for the rest of the company.
    d. Employees cannot access their work computer from home.

50. When an employee is promoted to a new position, what should be done with the system access in their new position?
    a. Nothing.
    b. It should be closed off.
    c. It is not an issue.
    d. It should be expanded; after all, the employee was promoted.

51. Who should notify accounts payable about an employee's departure, so accounts payable can notify the bank to cancel credit cards and signing authority?
    a. Controller
    b. CFO
    c. CIO
    d. HR

52. Which of the following is **not** considered a weak control practice?
    a. Using a petty cash box
    b. Returning checks to the requisitioner
    c. Using positive pay
    d. Allowing an unlimited number of rush checks

53. It is critical that accounts payable keep current on all of the following issues, ***except***:
    a. Best practices
    b. Investment opportunities
    c. New frauds
    d. New regulatory requirements for 1099s

¶1300 Fraud Prevention: General

Learning Objectives

Upon completion of this chapter, you will be able to:

Understand the importance of having a separate computer for online banking activities

Implement a mandatory vacation policy as well as a job rotation policy

Develop procedures for handling wire transfer information requests that do not enable fraud

Fraud is a sad fact of life, but one that everyone in the business world has to address. If they don't, crooks will take advantage. The term *business world* is meant to be inclusive of not only companies, but also colleges, universities, municipalities, not-for-profits, cities, states, associations, and other groups.

While there are still the stupid crooks out there, most of our readers will find they are dealing with a sophisticated and smart bunch of people who know how to manipulate technology for their own gain (and your loss). Hence it is imperative that every organization take appropriate action to protect their bottom line. What follows is a look at some of the best practices that will help protect your organization against the unscrupulous crooks trying to get their hands on our organization's money. They include:

Separate Computer for Online Banking
Wire Transfer Information Requests
Information on Internet for Vendors
Mandatory Vacation Policy
Job Rotation Policy
Handling Change of Bank Account Requests
New Verification Practices in Accounts Payable

¶1301 Separate Computer for Online Banking

The thieves involved in computer fraud are quite savvy. They are knowledgeable about how the banking system works as well as how to infiltrate your organization to get information that will allow them to take over your bank account. To do this, they find out who your employees are and what they do. With that, they can make an educated guess as to who does your online banking. Often, they are not quite sure, so they'll focus on several possible employees within your organization.

Once they've figured out who to hit, they send a targeted e-mail to those individuals. The e-mail will look legitimate, and their goal is to get the recipients to either click on the link or download the attachment. When the employee does that, a program is downloaded that enables the crook to capture the keystrokes made on the employee's computer. With that information, they are eventually able to figure out where you bank and a good user ID and password. With that information, they initiate an account takeover and initiate electronic payments from your account. This is also referred to as a *corporate account takeover*. Individuals have 60 days to notify their bank of unauthorized transactions and get their funds back. Everyone else has 24 hours.

Best Practice: Obviously, the best way to stop this type of loss is to prevent the account takeover. Not using a computer to access bank accounts is one way, but not realistic in this day and age. What is realistic is to set up a separate computer to be used for online banking only. It should not be used for accessing e-mails or surfing the web.

This inexpensive solution was first proposed by the FBI and the FDIC. Considering the cost of a stripped-down personal computer, it's really hard to understand why more organizations haven't adopted this simple best practice.

The best practice advice in this piece is meant to apply to both those who initiate the transactions as well as those who release or approve the transactions.

Almost Best Practice: None.

Special Pointers for Accounts Payable: Organizations that have adopted this practice need to make sure it extends to the person who releases the electronic payment transactions, both wires and ACH. Some busy executives have taken to releasing payments using their smartphones and/or personal tablets. While this by itself is not enough to cause a problem, many of these devices have not been outfitted with proper antivirus software. What's more, even if they have, few update this protection as often as it should be.

If your organization has adopted this practice, make sure you don't inadvertently undermine it. Make sure the PC is turned off as soon as the banking activity is completed. This way, no one will be tempted to use the PC when they're visiting the department. And under no circumstances should it be given to a temp to use because you have no other machine for the temp.

Worst Practice: Letting employees responsible for online banking activity use the same computer for banking activity as they do for downloading information from e-mails and clicking on questionable links.

¶1302 Wire Transfer Information Requests

This is an old problem that has persisted for many years. One of the pieces of information a crook needs to defraud your organization is your bank account number. This is especially true if the thief intends to produce phony checks. There are a number of ways to obtain this information, but the easiest is to call up and ask for it. Clearly, if the crook calls and asks outright for the account number, they won't get the information they want.

Instead, they call up and say they are making a wire transfer to the company and ask for the wire instructions. Of course, when it looks like money is coming to the company, most employees willingly provide the information. That's part of the reason many companies don't make payments from the account that receives wire transfers. Funds from that account are swept each night into a general account.

Best Practice: Don't give wire information to anyone who calls on the phone or e-mails asking for it. Now if you are wondering what would happen if this were a legitimate request, you are not alone. Most will provide this, but only to someone they already know at the company using a phone number, e-mail address, or fax number they already have on hand. Otherwise, they could be giving information to a fraudster.

Almost Best Practice: None.

Special Pointers for Accounts Payable: This is another reason why getting good contact information from your suppliers and keeping it updated is so important.

Worst Practice: Giving account information to anyone who calls and asks for it on the phone or by e-mail.

¶1303 Information on Internet for Vendors

The Internet is a wonderful thing. It makes disseminating information to those who need it simple, cheap, and effective. Unfortunately, crooks have figured out how to use the Internet to ferret out information about companies they wish to target as potential victims for their antics.

Best Practice: In the absence of fraud concerns (see special pointers below), post information on your Internet site that will help your vendors in transacting business with you. If possible, set up a secure portal where a user ID and password are required to gain access. With this security in place, you can post all your forms, a blank Form W-9, and Frequently Asked Questions (FAQs) focused on vendor issues.

If you routinely send out a New Vendor Welcome pack, it can be posed here as well. In fact, if you give new vendors access to this area, you can direct them to download the information rather than printing and mailing it. But take special care, for unless this information is protected so only vendors can view it, you may find yourself dealing with crooks taking advantage of the information you've posted.

Almost Best Practice: None.

Special Pointers for Accounts Payable: Special care needs to be taken when posting information on the Internet. While you might want to make your suppliers aware of certain facts, say that you are paying by ACH, you don't want to share that information with those who could use it to your disadvantage. Hence, unless you have a password-protected site for your vendors, think twice about posting your forms online so they can easily download them. Unfortunately, they won't be the only ones downloading your forms.

Worst Practice: Posting all information without any concerns over who might view it. This is especially troublesome if you are moving to electronic payments and have posted your sign-up form, where fraudsters can access it as well as your vendors.

¶1304 Mandatory Vacation Policy

You may wonder why we are writing about vacation policy in a course that is devoted to accounts payable. While on one hand vacation is an HR issue, it also can be an internal control point. The theory behind making employees take their vacation time is that in their absence, someone else would perform their jobs, and if any ongoing fraud was in progress, it would be uncovered in that timeframe.

Best Practice: Every person who has anything to do with the payment process (including invoice processors) should be required to take five (5) consecutive days off during which time someone else performs their job functions.

Almost Best Practice: None.

Special Pointers for Accounts Payable: Under no circumstances should the person be permitted to perform their job function from home. This completely defeats the purpose of having the person take their vacation time. As an added bonus, you will develop backup for positions that previously had no one trained to fill in, in case of emergency.

It is worth mentioning that if the task involves use of a password and/or user ID, a new one should be issued to the person filling in for the vacationing employee. Otherwise, it will be next to impossible to tell who did what. What's more, when the vacationing employee returns, the employee filling in could play havoc with your process and it would be impossible to tell who did what.

Worst Practices: Worst practices include:

Allowing employees to never take vacation.

Forbidding employees from taking too many consecutive days off.

Allowing employees to perform their jobs from home while on "vacation."

¶1305 Job Rotation Policy

There are many benefits to keeping the same person in the same job for an extended period of time. This is especially true when it comes to invoice processors. Not only does the employee get to know the job, but he or she gets to know the vendors and the contacts at the vendors. This comes in handy when there is a dispute or a special favor is needed from the vendor. Unfortunately, there is a big downside.

This affability can come back to harm your organization when your employee gets too friendly with an employee at your vendor. If the two of them get close enough and decide to help themselves to money that doesn't belong to them, they can collude to defraud your organization, and it will be a lot easier than if they didn't get along.

Best Practice: Wherever possible, rotate staff through different jobs on a regular basis. If possible, processors should not stay with the same accounts for more than six months. This prevents the type of hanky-panky discussed above. What's more, if they know they are to be rotated on a regular basis, they are less likely to try something funny; they'll know someone else will be taking over the account and looking over their work.

Almost Best Practice: If you can't manage the staff rotations every six months, try every year or two. If someone leaves, take advantage of that turnover to move people around, perhaps under the guise of promotions.

Special Pointers for Accounts Payable: An additional benefit from regular job rotations is that you will end up with a well-trained staff that can fill in for one another in case of unexpected emergencies or absences. You may get some resistance, especially the first time you try to implement a change, but stick to your guns. If you are having difficulty getting management agreement, your internal auditors will back you on this one.

Worst Practice: Allowing staff members to stay in the same position for years on end. This is especially poor if you also do not mandate vacations for the staff, as discussed earlier.

¶1306 Handling Change of Bank Account Requests

Most experts recommend that organizations pay as many vendors as possible using electronic payments, often referred to as ACH payments. And finally, the corporate world in the United States is following suit. Of course, most companies in other parts of the world have been paying their vendors this way for a long time. But that's another story. With this change come a few new issues. One of those is a variant on an old fraud. In the check world, from time to time, companies had to deal with fraudulent requests for changes in the remit-to address.

The electronic version, with its own unique twists, is fraudulent requests for changes to bank accounts used for payments.

Organizations change bank accounts all the time for a variety of reasons. Many times the old account is closed. Sometimes the company has changed its legal structure; sometimes it has changed banks. Occasionally, a fraud has occurred necessitating the change of account. Whatever the reason, when the change is made, if the organization has been receiving payments electronically, it notifies its customers of its new account. Most often, notification of this change comes in the form of an e-mail.

Unfortunately, crooks, often quite sophisticated in the use of the Internet, realize this is a potential gold mine. They spend a bit of time analyzing potential targets and creating quite legitimate-looking e-mails. These e-mails purport to come from the vendor, notifying customers of a change in the account where payments are being sent. As you might expect, the new bank account is one they control. Once money is sent to the account, it is quickly transferred out of the country, making recovery difficult. Regrettably, if your company falls victim to such an e-mail, it will still be on the hook for the payment.

Don't be fooled because the e-mail either looks legitimate or looks like it came from the vendor's e-mail account. Really smart IT folks can make the message look like it originated at the vendor's ISP.

Best Practice: An emerging practice that completely takes the onus off the customer is the use of automated self-service vendor portals, where the vendor is responsible for inputting its data, including bank account information for electronic payments *and* any changes to that information. This removes the onus from the customers. However, as this is being written, most organizations do not have such a portal, and therefore it is imperative that they do an independent verification of the request. This means contacting the vendor using information already on file to verify the change is a legitimate request. This also means regularly updating vendor contact information, something few companies do at this time.

Almost Best Practice: A few organizations now require that anyone requesting such a change supply not only the new bank account number, but the old bank account number as well. This makes it much more difficult, but not impossible, for a crook to perpetrate this type of fraud.

Special Pointers for Accounts Payable: This type of fraud is expected to grow in the coming years. It is a variant on the "change of remit-to address" letters crooks sometimes send. Those too should be verified, again using information you have on hand, not information included with the request.

Worst Practice: Just following the instructions in the e-mail or the letter without doing any verification that the request is legitimate. Equally bad is calling the phone number provided in the e-mail to verify the request. If it is a phony request, the person who answers the phone at the number provided will verify it is legitimate, when of course it is not. This is why keeping current contact information is so important.

¶1307 New Verification Practices in Accounts Payable

Apologies to ABBA fans who are probably gagging as they read this. The new "name of the game" in accounts payable should be *verification*. As best practices evolve to meet the growing threat from devious charlatans looking to defraud your organization in new and innovative ways, verification is emerging as the best practice way to stop them in their tracks.

It bears keeping in mind that many (but not all) of the individuals involved in these newer scams are quite smart, know the ins and outs of the Internet and banking better than most of us, and study social media for insights that help them create their diabolical tricks.

Let's look at a few of the changes best practice organizations are making to their accounts payable processes to ensure they don't get stung by one of these conniving frauds. Everyone should adopt them, as fraudsters don't discriminate on the basis of size, industry, or anything else.

New Best Practice #1: When setting up any new vendor in the master vendor file, check that vendor against the OFAC list. Yes, you still should be doing this check every time you do a payment run, but most companies don't. So, at a minimum, check at the very beginning of the relationship so you can cut off an unacceptable relationship before it has a chance to bloom.

New Best Practice #2: Check new vendor addresses against HR addresses to identify possible employees trying to set up a phony vendor. You won't find many matches, but when you do, make sure you research first because some will be false positives. But every once in a while, you'll find an employee playing games. By doing this before payments are made, you will be able to nip any fraud in the bud.

New Best Practice #3: Any request purporting to come from an existing vendor for either a change of bank account number or change of remit-to address should be verified by picking up the phone and calling a phone number you already have on hand. Be aware that while most of these phony requests come by e-mail, there have been reports of a few that arrived in a postal letter. Don't be fooled by that. The crook is just trying to lull you into thinking the request is a legitimate one.

Almost Best Practice #3: Some professionals complain that it takes too much time to call the vendor to confirm the request really came from them. Instead, they require that the e-mail requesting the change include some additional information, such as the old bank account number and/or details about the last two or three transactions. While this will certainly weed out some of the potential frauds, there is still a chance that a phony request could slip though.

New Best Practice #4: All wire transfer requests from CEO that arrive by e-mail should be verified by phone. Crooks have gotten quite good at spoofing CEO (and other high-level exec) e-mail addresses and doing it when they are difficult to contact. This is especially true if the request is marked *Urgent* or *Rush*.

New Best Practice #5: Whenever there is a request for a W-2 file or other sensitive employee information, verification should be mandatory. The IRS now recommends the following two steps: Two people review any distribution of sensitive W-2 data or wire transfers and the requirement for a verbal confirmation before e-mailing W-2 data. This includes when the CEO asks. In fact, in most organizations, the simple fact that the CEO is asking should trigger suspicion. Why would he or she want that information?

New Best Practice #6: Any time there is a request that is out of the ordinary in any way, separate verification should be required. This could include asking for some peculiar piece of information, change in a drop shipment location, or change having to do with payments. There have been all sorts of crazy requests, and a few people have fallen for them. Be very aware that crooks will spend whatever time they need studying your website and other social media sites so their requests look like they have inside knowledge when they really don't.

Special Pointers for Accounts Payable: It should be noted that the verifications we are discussing here should be either by phone using a phone number you already have on file or to an e-mail address you already have in your records. Do not respond to the e-mail requesting the change or information. Phone is by far the preferable method for this type of verification. If you don't have the phone number on file, search the Internet for the company's main phone number and work your way back from there. Yes, it can be a grueling task, but you don't want to put the company at risk by not doing it.

What becomes clear as we review the verification issue is that contact information in the master vendor file is more critical than ever. This is an issue many organizations ignore. And we're not just talking about collecting it in the first place, but also updating it on a very regular basis. For if we make that a standard part of our processes, when a vendor change of bank account request comes in, we can address it without too much time wasted looking for the right person. How good is the contact information in your master vendor file?

Worst Practice: Ignoring the issues discussed above, thinking they would never happen at your organization. That belief could cost your organization in a big way.

Review Questions

54. All online banking activity should be conducted on whose computer?
    a. Any computer, it doesn't really matter
    b. A separate computer used only for online banking
    c. The CFO's computer
    d. The accounts payable manager's computer

55. When wire transfer information is requested via a phone call, what is the best practice?
    a. Give it to the person calling.
    b. Ask the person for their e-mail address and e-mail it to them.
    c. Ask the person for their fax number and fax it to them.
    d. Don't give it out over the phone at all.

56. What is the best policy for posting vendor information on the Internet?
    a. Post all of it where everyone can view it.
    b. Don't put it on the Internet.
    c. Put it on the internet if you have a password-protected portal for your vendors.
    d. It doesn't really matter; it's not an issue.

57. In accounts payable, who should be required to take a mandatory vacation of at least five days?
    a. Everyone who has anything to do with the payment function
    b. No one
    c. Only those in management or supervisory positions
    d. Only those who process invoices

58. What is the best practice approach when a request for bank account change is made by a vendor currently being paid by ACH?
    a. Go ahead and make the change as requested.
    b. Call the phone number provided in the e-mail to verify the request.
    c. Ignore the request.
    d. Call or e-mail a contact using information currently on file.

¶1400 Fraud Prevention: Checks

Learning Objectives

Upon completion of this chapter, you will be able to:

Understand the importance of using positive pay

Implement strong controls around preprinted check stock

Integrate check fraud prevention practices into the accounts payable process

Check fraud, although it has been with us for a long time, still remains the most common type of attempted or actual payment fraud. Changes to the Uniform Commercial Code (UCC) have introduced the concepts of reasonable care and comparative culpability. Simply put, this means the person in the best position to prevent the crime will be held responsible.

Therefore, it is incumbent that all organizations take the appropriate steps to protect themselves against check fraud. In this chapter, we look at some basic tactics any organization should use, including:

Use of Positive Pay
Preprinted Check Stock Controls
Check Stock Storage
Other Check Fraud Prevention Practices

¶1401 Use of Positive Pay

Positive pay is the best protection any organization can use to protect itself against check fraud losses. It is a product offered by most banks that requires companies using the product to produce a tape that is sent to the bank each time there is a check run. The tape contains a list of check numbers and dollar amounts. As checks clear, the bank reviews the list before clearing each check to ensure the item is on the list. Once the check has been presented, the item is removed from the list.

If an item is not on the list, the bank will either reject it or call the company, depending on the arrangements made when the product is set up. Those who issue frequent manual or rush checks are advised to get the calls as these items sometimes don't end up on the positive pay file. Clearly, the company is advised to add them to the positive pay file when sending them to the bank, but these items often occur between check runs, resulting in a reporting delay.

It is important to keep in mind that check positive pay does not protect against all types of payment fraud, only check fraud. Many of the crooks who operate in the fraud world are very smart and very sophisticated with technology. Do not underestimate them.

Best Practice: Use payee name positive pay, if your bank offers the product. This is the latest development in an evolution of this fraud deterrent that has arisen as crooks find ways to manipulate the banking system. Once they understood the mechanics of the positive pay product, some of the smarter ones realized the only facet of the check that could be altered was the payee name. So, that is precisely what they did.

To counteract this new threat, banks developed the aforementioned payee name positive pay. Companies using that product also include the payee name on the file sent to the bank for matching before payment.

Almost Best Practice: For those using a bank that does not offer payee name positive pay, then the plain vanilla positive pay is the best choice. For those organizations that do not have the capability to produce a file for the bank, reverse positive pay is their best option.

Reverse positive pay requires the company to get online every day and verify the checks being presented for payment. If there is an item they wish to reject, they must notify the bank, usually by one o'clock. Whether no action means pay or not to pay depends upon the arrangement established with the bank. Use of reverse positive pay also means the company must have an employee verify transactions every day the bank is open, even if it is a vacation day for the company.

Special Pointers for Accounts Payable: Again, keep in mind that positive pay only protects against check fraud. Savvy criminals have figured out that they can represent positive pay rejects as ACH debits and still get their hands on your money. This is just one of the reasons that forward-thinking professionals realize that while positive pay is important in the fight against fraud, it is just one tool in an arsenal used to combat this insidious crime.

It should be noted that if you are verifying transactions every day using reverse positive pay, you are in effect doing a daily bank reconciliation. As you will see in other sections on fraud, daily bank reconciliations are now considered essential in the war against payment fraud.

Finally, positive pay exceptions should be handled by someone not involved in any other leg of the procure-to-pay function. For many organizations these calls from the bank are handled outside accounts payable. This ensures that if any hanky-panky is going on with someone involved in making payments, they don't have the "opportunity" to hide the problem, when the bank calls.

Worst Practices: Worst practices include:

Not using any type of positive pay.

Not doing bank reconciliations on a regular basis.

Ignoring the check fraud issue, thinking it would never happen in your organization.

¶1402 Preprinted Check Stock Controls

Check stock for paper checks has come a long way. A good portion of the corporate world has already stopped using preprinted check stock. These are checks preprinted with the company name, bank information, and perhaps the corporate logo. However, they still remain in use by some reading this. Those who rely on preprinted check stock need to do everything they can to make those checks difficult to forge. For this reason, safety features need to be incorporated into the check stock. Some of those features include:

Watermarks. Watermarks are subtle designs of a logo or other image. Designed to foil copiers and scanners that operate by imaging at right angles (90 degrees), watermarks are viewed by holding a check at a 45-degree angle.

Microprinting. A word or a phrase is printed on the check so small that to the eye it appears as a solid line. When magnified or viewed closely, the word or phrase will become apparent. Copiers and scanners can't reproduce at this level of detail, so microprinting when copied will appear as a solid line.

Laid lines. Laid lines are unevenly spaced lines that appear on the back of a check and are part of the check paper. This design makes it difficult to cut and paste information such as payee name and dollar amount without detection.

Reactive safety paper. This paper combats erasure and chemical alteration by "bleeding" when a forger tries to erase or chemically alter information on the check, leaving the check discolored.

Special inks. These are highly reactive inks that discolor when they come into contact with erasure chemical solvents.

Color prismatic printing. This type of printing creates a multicolor pantograph background that is extremely difficult to duplicate when using a color copier or scanner.

Special borders. These borders on the check have intricate designs that, if copied, become distorted images.

Warning bands. Warning bands describe the security features present on a check. These bands alert bank tellers or store clerks to inspect the check before accepting it. They may also act as a deterrent to criminals.

Thermochromic inks. These are special, colored inks that are sensitive to human touch and, when activated, either change color or disappear.

Toner grip. This is a special coating on the check paper that provides maximum adhesion of the MICR toner to the check paper. This helps prevent the alteration of payee or dollar amount by making erasure or removal of information more difficult.

Best Practice: Get rid of your preprinted check stock by moving as much as possible to ACH (electronic payments) and p-cards. Clearly, you will need good upfront controls to ensure your payments are appropriate and not duplicates.

For those items that cannot be paid with one of those two mechanisms, consider printing checks as needed on a laser printer. Obviously, you will need to build in the appropriate controls in the process and incorporate a facsimile printer that produces the check with a signature.

Almost Best Practice: If you use preprinted check stock, it is recommended your check stock include at least three safety features. These make it difficult, although not always impossible, for a fraudster to copy your checks. More than three is certainly acceptable, but if you want to be seen as exercising reasonable care, three is the minimum you need.

Special Pointers for Accounts Payable: Preprinted check stock is fast going the way of the buggy whip, electronic calculators, and VCRs. But as long as you are using it, it is imperative that it contain the requisite safety features.

Worst Practice: Purchasing the cheapest checks possible without regard to the incorporation of safety features. This makes it incredibly easy for the crook who manages to get hold of one of your checks. Replicating it is child's play, and when those phony checks hit the bank, your organization won't be deemed as exercising reasonable care.

¶1403 Check Stock Storage

It's well known that banks rarely, if ever, verify the signature on a check. So, if your preprinted check stock is not held in a secure location, you could be increasing your chances of check fraud. Anyone getting their hands on one of your checks could simply fill it out for whatever amount they chose, sign it, and if your organization doesn't use positive pay, cash it. Even with positive pay, blank checks present a real and serious problem if they end up in the wrong hands.

Best Practice: Preprinted check stock should be stored in a secure location that is locked. Access to that location should be limited to one or two people. When setting up your workflow, keep the appropriate segregation of duties in mind when assigning responsibility for the check stock. Ideally, it should be with someone who has no signing authority and does not process invoices. There should be no exceptions.

If the check stock is held in a storage closet, as it sometimes is, the key to that storage closet should not be given out randomly to anyone who might need to get something from the closet. That's why many organizations use a locked file cabinet in the locked storage closet to hold blank check stock. If they want to be really careful, the person who has the key to the locked file cabinet does not have a key to the storage closet.

Almost Best Practice: None.

Special Pointers for Accounts Payable: Sometimes companies keep a spare checkbook around for rush checks or unexpected employee separations. While they keep the rest of the check stock in a secure location, this checkbook might be kept in a manager's desk or a file cabinet in a highly trafficked area. Even if the file cabinet is locked, the key is often left in the top drawer of a nearby employee's desk. Unfortunately, this undoes a lot of the controls of storing the rest of the blank checks properly. Yes, it is much easier to have ready access to the checks for emergencies, but it also introduces a level of risk that far outweighs the ease factor.

You should also keep a log showing how many checks were printed in each check run, the beginning check number, and the ending check number. If you need any checks for alignment before printing, these need to be accounted for on the log as well. Finally, if any checks are damaged, they need to be accounted for in the log as well. The log should be periodically audited by a party not involved with the check production process.

The damaged checks should be kept in a folder. They should be marked *VOID* across the front if there is any chance they'd be useable, and the signature block should be ripped or cut off.

Worst Practices: Worst practices include:

Not locking check stock.

Ignoring segregation of duties issues.

Giving access to the closet where the check stock is stored to numerous employees.

¶1404 Other Check Fraud Prevention Practices

Protecting the organization against check fraud is a multifaceted job. Companies not only have to do everything they can to prevent the fraud from happening, they also need to sleuth out those instances when a fraud manages to get through their controls.

Best Practice: Other check fraud prevention best practices include:

Don't return checks to requisitioners.

Ensure that vendor complaints and discrepancy reconcilements are directed to staff who are separate from the invoice processing staff.

Deliver checks to the mailroom at the end of the day.

Minimize, if not eliminate, all rush checks.

Establish appropriate procedures for uncashed checks to ensure proper reporting for unclaimed property.

Establish a separate account for refunds.

When an authorized check signer leaves the company, immediately notify the bank of the cessation of his or her signing authority.

Almost Best Practice: Implement as many of the best practices described above as possible. These should be integrated into your comprehensive fraud prevention routines.

Special Pointers for Accounts Payable: Sometimes, despite your best efforts, a fraudulent check slips through. One of the ways to get an overview of your organization (at no cost) is to hire a duplicate payment audit firm to recover any duplicate or erroneous payments your organization may have made. As part of that effort, you should receive a comprehensive report identifying weak points in your process. Don't overlook this important report.

Finally, as we've mentioned several times already, many of the crooks involved in payment fraud are quite smart and knowledgeable about the banking community. They continually look for ways to circumvent controls. Unfortunately, they are often successful. When this happens, the banking community often develops a new control or product to guard against the new fraud.

The only way for you to protect your organization on an ongoing basis is to keep up to date on the newest frauds and the products and strategies available to protect your organization. This should be an integral part of any professional's job, especially if they are involved in the payment arena. The best practice plan you put into effect to protect your organization today may need to be updated in six months or a year. So, don't rest when it comes to fraud prevention and detection. It's an ongoing battle—but one you can win, if you put in the necessary time and effort.

Worst Practices: Worst practices include:

Using a rubber stamp to stamp on the signature.

Giving the rubber stamp to an admin to "sign" a pile of checks.

Signing blank checks and leaving them with an admin to handle emergencies.

Review Questions

59. Which of the following represents a best practice when it comes to the use of positive pay?
    a. It is not a best practice to use positive pay.
    b. Use payee name positive pay, if available.
    c. Use of positive pay is a worst practice.
    d. It is neither a good nor a bad practice to use positive pay.

60. Which of the following represents a best practice when it comes to preprinted check stock?
    a. There is no best practice related to use of preprinted check stock.
    b. Get rid of preprinted check stock.
    c. Use of preprinted check stock is a best practice.
    d. Preprinted check stock does not need special storage.

61. Preprinted check stock should be stored in which of the following manners?
    a. In a secure locked closet
    b. In a file cabinet
    c. In a desk drawer of an unlocked desk
    d. Near the printer for ease of use

62. Which of the following will help prevent check fraud?
    a. Returning checks to requisitioners
    b. Delivering checks to the mailroom early in the day
    C. Using positive pay
    d. Allowing as many rush checks as wanted

¶1500 Travel and Entertainment Policy

Learning Objectives

Upon completion of this chapter, you will be able to:

Create a strong travel and entertainment policy that is compliant with IRS guidelines for the entire organization

Develop procedures for verifying data and handling receipts

Understand why organizations are moving towards requiring the detailed meal receipt

Identify policy violations the detailed meal receipt might uncover

The travel and entertainment (T&E) policy is any organization's first line of attack when it comes to getting its employees to conform to a set of rules of behavior and preventing fraud. This chapter delves into this issue in some depth, focusing on the following:

Formal Policy
Expense Report Form
Verifying Data
Handling Receipts
Detailed Meal Receipts

¶1501 Formal Policy

The T&E policy should spell out the guidelines for company employees when it comes to travel and entertainment. It details some or all of the following:

What receipts are required
What is allowable
What is not allowable
How documentation should be submitted
What approvals are necessary
Timing of reporting
If cash advances are permitted and, if so, under what circumstances
If corporate T&E cards must be used
Reimbursement policy
What hotel chains are preferred or required
What airlines are preferred or required
What car rental agencies are recommended or required
Whether employees must stay over on a Saturday night if a lower fare can be obtained
How unused tickets are to be handled

Best Practice: The organization's T&E policy should be formal, written, and distributed to all employees for easy reference. It should be updated periodically, no less frequently than once a year. Ideally, the update should take place every time a change is made.

Companies have eliminated all printing costs by publishing the T&E policy on the corporate intranet site or creating a PDF file. In this way, updates can be communicated quickly and the policy shared with everyone who might need access to it. Cost is simply not a consideration.

Whenever there is a major change to the T&E policy, a memo should go out from a senior executive explaining the change. The notice should be sent to all employees.

For a T&E policy to be effective, it has to be enforced across the board. This means that managers should not be allowed to override the policy, where they think it does not apply to their staff. Obviously, for the policy to be effective it also needs to be adhered to by executives at all levels.

Companies using an automated system can have a policy compliance feature built in. In these systems, reports that are in violation of the company policy are flagged for further investigation. The AP department can then return these reports to the approver's supervisor for further review.

Some of the more advanced automated systems take policy compliance one step further. They refuse to allow the submission of reports in violation of the policy. This is a bit extreme, as there will infrequently be occasions when an expense outside the policy is justified.

New employees should be given a copy of the T&E policy as part of their welcome packet. Ideally, there should be a focal point for questions relating to the T&E policy.

Frequent T&E policy violators should be noted and their reports checked thoroughly each time one is submitted. (See the "Verifying Data" section later in this chapter.)

Senior management must support the policy in a very public way. Some companies do this effectively by having either the chief executive officer (CEO) or the chief financial officer (CFO) sign the cover memo that goes out with the policy. Others do it by having one of these senior officials sign a memo about T&E policy compliance that is put in the front of the T&E policy manual.

Almost Best Practices: None. There is no reason for a copy of the policy not to be given to every employee. Cost of production is no longer an issue.

Special Pointers for Accounts Payable: Processors should be given the right to question any item on any report, no matter how senior the executive whose expense report is under scrutiny.

Do not rely on the common sense of your employees. You will quickly find that you have a few whose idea of what is reasonable for business travel does not mesh with the corporate policy. In order to avoid unpleasant confrontations in this situation, make the policy as detailed as possible so there can be no misunderstanding.

No matter how good you are about educating employees about the T&E policy, via e-mail updates, memos, copies of the manual, and the Internet, calls will still come into AP about the policy. Additionally, violations will continue to appear on T&E reimbursement requests. A few flagrant violators will continue to claim, "Nobody told me that," regardless of the vigilant efforts of the AP education team. The goal should be to wear these people down, forcing compliance through whatever means the company's policy allows. This can sometimes mean refusing to pay for flagrant policy violations—but only with very senior management–level support!

Worst Practices: Worst practices include:

Uneven enforcement of the policy, which can lead to additional violations and higher costs.

Not having a detailed policy.

Not giving a copy of the policy to every employee.

¶1502 Expense Report Form

There has been quite a bit of innovation and consolidation in the last few years in the area of expense reporting. Several of the companies providing third-party services have merged. SaaS (software-as-a-service) models have emerged, which effectively translate to a pay-as-you-go approach. And, of course there has been the emergence of cloud technology, advanced mobile devices (both smartphones and tablets), and continued increased corporate scrutiny on expenses. Yet despite these advances, Excel spreadsheets still remain a key player in the expense reporting arena, especially where small and midsized companies are concerned.

Best Practices: Any automated form, whether it be created on a system purchased from a third party or developed in-house, can be e-mailed first for approvals and then to AP for submission. This makes the process much smoother and provides tracking information for those who want to know the status of their expense reports, reimbursements, and travel card payments.

If the form is automated, policy compliance can be incorporated in some of the more advanced systems. This is ideal, especially at a large company. It also takes the burden off the AP staff, who really should not have to monitor for policy compliance. By having the system flag policy violations, the company can take appropriate action with offending employees to bring them into compliance.

Reporting can also be done to aggregate where funds are being spent. This information can then be used to negotiate better rates with preferred suppliers.

It should be noted that when we talk about policy violations, we do not necessarily mean outrageous spending. A violation could be something as simple as not flying on the preferred carrier, not using the company travel agent, or not flying the cheapest route because it meant stopping over and losing an additional day's work time.

Some of the third-party models offer an interesting array of features. One that we like best is the incorporation of a link to the Internet that verifies miles driven, when an employee is asking for reimbursement for use of a personal vehicle. This software takes the addresses involved and calculates the actual mileage driven. We suspect this has put an end to some petty cheating that was probably going on in a few instances, where such verification was not available.

Almost Best Practice: If a third-party system is not used, at a minimum, the forms can be e-mailed for approval. The automated form should incorporate locked formulas. There is really no reason why employees should print out expense reports and attach their receipts before giving the reports to the supervisor for approval. If the supervisor wishes to see the receipts, he or she can ask for them or, if the receipts are scanned, automatically look at them online.

Special Pointers for Accounts Payable: There will always be employees who don't fill out their forms correctly, don't do the appropriate coding, don't do the math (or do it wrong), use old T&E forms, and so on. Each time this happens, take the opportunity to try and educate the offending employee.

Homegrown automated forms, typically developed using Excel spreadsheets, should have formulas embedded in the worksheets so the employee does not have to do the math. This eliminates the mathematical errors. The formulas can be locked, preventing the employee from tampering with the evidence. Some of these in-house–developed forms are advanced and work perfectly fine for even rather large midsize companies.

Worst Practices: Worst practices include:

Use of paper forms.

Use of an Excel spreadsheet without locking formulas.

¶1503 Verifying Data

There's a saying in T&E about "not spending a dollar to find a dime." It refers to the practice of checking every single T&E report in detail to ensure that no employee has charged something to the company that he or she is not entitled to. Some companies still feel the need to do this. This issue relates closely to corporate culture.

It should be noted that a third-party automated expense reporting system (or an in-house model) can effectively check 100 percent of the transactions, without additional cost.

The problem of managers approving expense reports without ever looking to see what they are signing continues. The problem with this approach, as you probably realize, is that after a while the employee realizes the manager doesn't look, and a few decide to push the envelope with what they submit for reimbursement. Occasionally, it gets really out of hand.

Best Practices: Assuming you are not using a third-party system that automatically verifies each report, you will need to balance your verification requirements against the resources available to handle the task. Randomly selected expense reports should be checked in detail. The percentage of reports selected can range from 5 to 25 percent, depending on the corporate tolerances. Additionally, reports from the following should be reviewed completely each time they are submitted:

Known offenders and rogue spenders

Any report that contains a policy violation

Any report over a certain high-dollar amount, say $10,000

This practice is referred to as spot-checking. Ideally, you will be scanning reports, so you can view this information online. If not, this will entail getting the receipts, if attached, or retrieving them if mailed in a separate envelope and verifying that all are included on the report.

Policy violations should be run by the submitter's supervisor for approval, even if the report is approved. Serious violations should be taken at least one level higher.

There is a growing practice of making managers responsible for the reports they approve. While a very few organizations have adopted (and enforced) a policy of firing managers who approve a reimbursement request for something that is flagrantly out of compliance with the policy, most are not willing to go that far. However, a more measured approach is to make this lack of managerial oversight part of the annual review, dinging the manager's annual increase if he or she has failed to properly monitor a subordinate's expense reimbursement requests.

Almost Best Practices: In some organizations, there is corporate resistance to spot-checking. Assuming the company in question has not gone to an automated system where expense reports would get 100 percent review, there is a halfway approach. Companies that want to go the spot-checking route often start by verifying the data on half of the reports, for example, and then working their way down to a lower level. This is a good way to start the process for those companies wanting to change the way they verify the data on the expense reports.

Special Pointers for Accounts Payable: Some organizations, especially those that want to set a tone of compliance from the top, will insist that all reports of all C-level executives be checked every time.

In theory, expense reports are reviewed by the submitter's supervisor and approved by this individual. The approver signs the report, indicating that he or she has checked everything and reimbursement is okay. The reality is that many supervisors don't review the reports and simply sign them without even glancing at them. This is especially true of higher-level executives as well as those in high-paying fields, such as traders, stockbrokers, and the like. Thus, sometimes checking reports is required and will not make AP popular with those whose reports are being checked.

Worst Practice: Not checking reports at all.

¶1504 Handling Receipts

When an employee completes an expense report, he or she must verify those expenses by providing receipts. The IRS guidelines require receipts for expenditures in excess of $75. Despite the fact that the IRS instituted this limit in 1995, very few companies have followed their lead. In fact, we are seeing a growing number of organizations that now require all receipts. This is in stark contrast to the past when most organizations required receipts only when expenditures were in excess of $25.

The other issue regarding receipts is how they are sent to AP. A growing number of companies are now scanning receipts, even if they don't use a third-party automated expense reporting process.

Best Practices: There has been much dialogue around this issue, and the growing practice seems to be that companies are now requiring all meal receipts as well as receipts over a certain dollar level for other expenditures.

When receipts are submitted to AP, they are either scanned or sent in specially coded envelopes. They should not be attached to the reports, from which they can easily become separated.

If receipts are scanned, employees should be required to hold on to the originals for 90 days. This gives the processor time to handle the report, spot-check receipts, and—if they see something that doesn't look right—request the original receipt.

Periodically, even if nothing is wrong, the original receipt should be requested. This is to let the staff know the receipts are being reviewed and hopefully will serve as a deterrent to anyone thinking of playing games with their receipts.

Almost Best Practices: If receipts are not sent separately, get rid of those pesky little pieces of paper. Insist that they be taped to a larger piece of paper. Ideally, all will fit on one piece of paper. A company that sets the limit at which receipts must be submitted at either $25 or $75 should not have many little pieces of paper. Companies that set that limit at $5 can get tons of these little receipts submitted.

Of course, as credit cards continue to grow in popularity, there will be fewer questionable receipts. And, if corporate travel cards are used, this too will make a dent on the issue.

Special Pointers for Accounts Payable: Regardless of the dollar level set by the company, be aware that there will be employees who will insist on submitting receipts for every last cent they spend.

Worst Practices: Worst practices include:
Verifying every receipt manually.
Not looking at any receipts.

¶1505 Detailed Meal Receipts

Most restaurants, especially if you pay with a credit card, provide not only a receipt for your records but a detailed meal receipt. When submitting documentation for expense reimbursement purposes, the receipt showing the amount plus the tip is what was traditionally used.

However, a growing number of companies now require that the detailed meal receipt be turned in as well. From this, the person reviewing the expense report can determine:

If liquor was ordered when the policy prohibits reimbursement for liquor
If an inappropriate amount of liquor was ordered
How many adults were at the meal
If kiddie meals were ordered
If something (mainly gift cards) was paid for in addition to the meal

Unfortunately, there have been numerous instances where all of the above have been included in expense reimbursement requests. Without the detailed meal receipt, it is possible to mask the inappropriate purchases.

One would hope that if the detailed meal receipt is required, employees would be smart enough to avoid the types of behavior described above, as well as any other shenanigans they might dream up. Thus, requiring the detailed meal receipt serves more as a deterrent than a tool to actually find fraud—or at least, one would hope the requirement would deter that type of inappropriate spend.

Best Practice: Require but spot-check meal receipts with expense reimbursement reports to verify policy compliance and non-inclusion of gift cards and other items not normally reimbursed on expense reports.

Almost Best Practice: None.

Special Pointers for Accounts Payable: Sometimes when someone hears about the requirement to get the detailed meal receipt for every meal, they start to question the appropriateness, given the extra work verifying those receipts is likely to create. The important issue is that not every meal receipt will be checked. For the most part, they are to be spot-checked like other receipts. Of course, if you have your list of known expense reimbursement abusers, verify all their receipts, all the time.

Worst Practice: Allowing the expense to be documented by either the detailed receipt or the receipt showing the total payment. This opens the door for the receipt to be submitted twice, perhaps by two different employees.

Review Questions

63. How frequently should the travel and entertainment policy be updated?
    a. It doesn't need to be updated.
    b. Whenever there's a change.
    c. Whenever the CFO indicates it should be updated.
    d. Whenever there is a change on the board of directors.

64. In an ideal situation, how are policy violations handled during the expense reporting process?
    a. They are ignored.
    b. They are not an issue at most organizations.
    c. They are flagged for further review.
    d. They are flagged, but no one reviews them.

65. When it comes to checking details on expense reports, the recommended best practice is which of the following?
    a. 100 percent of all returns be checked.
    b. Spot check 5 percent to 10 percent.
    c. Only check the expense reports of sales.
    d. No checking is necessary; managers should do that.

66. The IRS requires that organizations have receipts for all expenditures over what dollar limit?
    a. $10
    b. $25
    c. $75
    d. $1

67. Why are a growing number of companies now considering getting the detailed meal receipts from employees putting in for expense reimbursements for those meals?
    a. It is an IRS requirement.
    b. It is required by Sarbanes-Oxley.
    c. To determine if dessert was ordered.
    d. To determine if what was ordered conforms to the policy or if there was fraud.

¶1600 Travel and Entertainment Issues

Learning Objectives

Upon completion of this chapter, you will be able to:

Understand why cash advances are counterproductive for the accounts payable function

Develop policies for handling travel issues created when employees leave

Create an efficient and effective policy for reimbursing employees for travel expenses

Travel and entertainment has a lot of issues associated with it and all need to be addressed carefully or chaos will ensue. In this chapter, we take a look at the best practices associated with:

Cash Advances
Unused Tickets
Departing Employees
Making Travel Reservations
Reimbursing Employees
Reimbursing for Items Paid for with Points

¶1601 Cash Advances

Before corporate credit cards were commonplace, employees would routinely pay for all their travel expenses themselves. Airline tickets had to be booked and paid for weeks, if not months, in advance. Upon completion of a trip, employees would submit their expense report to obtain their reimbursement, as they do today. The difference was that traveling employees could be out-of-pocket for significant amounts of money, especially if they traveled frequently to foreign countries or first class.

Thus, the practice of cash advances evolved. To help the financially overburdened traveling executive, companies would advance them some amount of cash to cover these expenses. Upon the completion of the trip(s) and the expense report, the two would be reconciled and a settling up would occur. More often than not, this entailed the employee writing a check for the amount he or she owed the company. If you are sitting there scratching your head, consider the following facts:

There usually were no limits on the cash advance.
There was no interest charged on the cash advance loan.
Interest rates for the last 10 to 30 years were high (or very high) compared with today's rates.
Few employees are willing to pay out-of-pocket when their employers offer a no-cost alternative—the cash advance.

Clearly, not all employees abused the cash advance system. Nothing could be further from the truth. However, some employees who have to return part of the advance frequently drag their feet in completing their expense reimbursement reports. This exacerbates the already problematic issue of getting all employees to complete their reports on time.

The other factor affecting cash advances is that, in a few cases, employees are tempted to fabricate expenses to justify not returning the cash.

Finally, there are the financial implications and procedural inefficiencies of the cash advance process. In higher-interest-rate environments, the lost interest income or the increased borrowing costs associated with cash advances were a factor. Even today, in a relatively low-interest-rate situation, there are cash flow implications. When cash advances are used, they have to be accounted for correctly and issued in the form of either cash or checks. Neither process adds value.

Best Practices: Don't give cash advances. Not every company is willing to take the "just say no to cash advances" stance. It may go against the corporate culture, or it may not be feasible given the level of employees who are asked to travel on the company's behalf. If advances are given, they should be given

only under special circumstances, with the approval of both the individual's direct supervisor and the supervisor's supervisor. Make it difficult, not impossible, so people will seriously consider before asking for an advance.

If a cash advance is provided, do it in the form of an electronic (ACH) payment. Giving cash advances in the form of cash is rife with procedural issues and can lead to abuses.

Special Pointers for Accounts Payable: Realize that if you have new employees just out of school who are required to travel, you may have to give them cash advances as they may not be able to fund the trips themselves. This is especially true if your organization does not offer its employees a company-paid travel card.

Worst Practices: Worst practices include:

Routinely giving cash advances.

Not following up with employees who receive cash advances to make sure expense reports are submitted on a timely basis.

Using cash for cash advances.

Not using a consistent policy for cash advances.

¶1602 Unused Tickets

The plans of business travelers change frequently. The result is unused tickets. With paper tickets, at least travelers have the piece of cardboard to remind them that the ticket was not used and can be either exchanged for another ticket or refunded. With e-tickets, this reminder is not available. Since many business travelers now purchase nonrefundable tickets, they are then faced with a ticket that can be used only against future travel and not refunded. Thus, it is necessary to keep track of these tickets.

Even if the ticket can be refunded, someone must take the necessary steps to get the refund. In the past, travel agents helped get these refunds. With few organizations relying on travel agents, the task now falls to the individual traveler or perhaps the admin within the department. If no action is taken, the ticket will expire (typically within one year) and be worthless.

This is an issue that should be considered when booking travel. Instead of automatically purchasing the cheapest ticket, some consideration should be given to whether the trip is likely to be canceled. If this is the case, consider buying a refundable ticket and paying the price. Sometimes, the price difference is small. This is especially important if the employee in question is not someone who travels frequently.

Best Practice: A formal procedure should be put in place to handle unused tickets. American Express says that more than 4 percent of e-tickets issued by corporate travel departments go unused. New systems have emerged to track unused e-tickets and even process refunds; however, many companies are unaware of these systems.

If you use a third-party expense reporting system, talk to the service provider to see what options it has for tracking unused tickets. Make sure to activate that feature, if it is available.

Almost Best Practice: Have someone in the travel office or department track the status of unused tickets and send reminders to travelers who have them.

Special Pointers for Accounts Payable: Unused tickets will be an issue as long as company employees travel. Find some system to track them; otherwise, even the most conscientious travelers will forget about them.

You might also want to make sure your employees understand what a non-refundable ticket is. A few think it means that if the ticket isn't used, it is lost. This is typically *not* what the airlines mean. They mean you can't get the money back for the ticket. You can use the funds to purchase another ticket on the same airline within a set period of time, usually one year. You may have to pay a change fee as well. But at least the entire amount won't be lost.

Worst Practice: Doing nothing. Unused tickets are an unnecessary drain on the corporate cash flow and impact its profitability in a negative way.

¶1603 Departing Employees

From time to time, every organization will lose some of its employees. Some will leave of their own accord and others depart at the invitation of the company. The cause for the departure does not matter. The result is the same.

Sometimes people are lulled into a false sense of security if a seemingly content employee leaves for a new job. They think there is no risk. Most of the time, this is true—but not always. And of course, it is impossible to identify those instances when it is not. So, like virtually every other issue discussed in this work, there should be no exceptions when it comes to the application of best practices.

Best Practice: When employees leave, the following should occur:

They should turn in their last expense report before leaving.

They should return any excess cash advances, if they were given any.

If you put the employee in your master vendor file for expense reimbursement purposes, immediately deactivate the employee.

They should turn in their travel and entertainment credit card.

The card administrator or accounts payable should be notified of the termination immediately so they can take appropriate steps.

The bank should be notified to cancel the credit card immediately.

Almost Best Practice: If you cannot manage to get this information on a timely basis from HR, periodically get a list of active cardholders from your bank. Match it up against the list of current employees and terminate any cards held by people not on the list of current employees.

Special Pointers for Accounts Payable: For this practice to work, there must be coordination between HR and accounts payable. It is not enough to simply get the card back. It must be canceled at the bank. If the employee is devious, he or she will have written down the card number, expiration date, and security code.

Even if he or she intends no malice, trouble can occur if the former employee continues to carry your credit card around in his or her wallet. The former employee can inadvertently use it, or worse, if the former employee's wallet is stolen; your card will now be in the hands of thieves. When the individual reports lost credit cards to the various issuers, it is almost certain he or she will forget about your card. Get the card back. Don't leave it around where they can only cause problems.

Worst Practice: Not doing anything about travel and entertainment issues as they pertain to departing employees.

¶1604 Making Travel Reservations

Until approximately ten years ago, companies routinely required employees to book their travel arrangements through preapproved travel agencies. Larger companies negotiated special rates, based on volume usage, with airlines, hotel chains, and car rental agencies. Many big organizations continue to negotiate preferred rates.

The Internet has changed a lot of this. Employees routinely surf the Internet, finding lower airfares and hotel rates than are being offered by the corporate plan. Until recently, the prevailing wisdom was to stick with the corporate rate because, overall, the company gained more, due largely to the volume discounts offered by such plans.

Now e-commerce sites like Expedia and Travelocity have developed their own electronic equivalents of the old corporate travel office. The features they offer emulate common off-line travel services. And while these plans are not free, they are not expensive either.

Best Practice: Employees can either book on their own or through a corporate initiative, whichever the travel policy dictates. In either case, they are to:

Get the best price, taking into account whether the ticket might need to be canceled.

Ensure policy compliance.

Use airlines and hotels where preferred rates have been negotiated.

Almost Best Practice: None.
Special Pointers for Accounts Payable: If the company policy requires use of an agency or certain airlines or hotels, expect complaints from employees who find better rates. One way to try and limit the time spent on this issue is to include a page in the travel policy explaining the rationale for the use of the preferred carrier/hotel/car rental agency. Then when people complain, you can point them to the page for a "full explanation." This works particularly well when a high-level executive has endorsed the policy in writing on one of the first pages.
Worst Practice: Having no policy regarding reservations.

¶1605 Reimbursing Employees

Employee reimbursement can be handled in one of several ways. These include:

The employee being given a check
The employee having a check mailed to his or her house
Have the reimbursement included in the employee's paycheck
Have the reimbursement direct deposited along with payroll
Have the reimbursement direct deposited to a bank account

This seemingly innocuous task can create havoc in AP departments that insist on using payroll-related reimbursements. A few employees use their T&E reimbursements as "mad money," not sharing this money with their spouse. These individuals will cause quite a stir if the proposal is made to either include the reimbursements in a paycheck or have the funds direct deposited to the account where the paycheck is deposited.
Best Practice: Mandate that T&E reimbursements be direct deposited to an account, but allow employees to direct the funds to an account other than the one where payroll is deposited. By adding the flexibility feature, the number of arguments will be reduced. It is beyond the responsibility of any company to address the issue between spouses.
Almost Best Practice: None.
Special Pointers for Accounts Payable: If employees insist on a check and management tolerates this, look for opportunities to get them to try the direct deposit feature, for example, when reimbursement is late and the employee needs the funds.
Worst Practices: Worst practices include:

Reimbursing by check.
Allowing employees to pick up reimbursement checks from accounts payable.

Both are an extremely inefficient use of the AP staff and cause problems when checks are misplaced or picked up by admins. Additionally, communication snafus between executives and their admins sometimes lead to a request for a second check when the first is lying on someone's desk.

¶1606 Reimbursing for Items Paid with Points

This appears to be a growing trend, and therefore should probably be addressed in all policies. Some employees have been accumulating points and then using them to make reimbursable purchases. They then request reimbursement of the cash value of the purchase. While this practice isn't widespread—yet—we did hear from several readers who have encountered such requests.
Best Practice #1: Don't permit this. This issue should be addressed in the policy. If it isn't, the door is left wide-open for any employee to use their points and ask for reimbursement. When we asked readers in our ezine about this course of action, they were all adamantly against reimbursing under these circumstances. Here is one simple statement one company added to its organization's travel policy:

> Credits such as gift cards, airfare credits and frequent flyer miles, whether earned on personal or business travel, are not reimbursable as there is no cash outlay for such a transaction.

Best Practice #2: There is another step every organization can and should take to eliminate even the possibility of such a request. Mandate the use of a company card for all purchases and travel, no exceptions. Here is the policy used by one such organization:

> All approved travel, seminars, conferences, professional dues, books and subscriptions, etc. are to be paid on the corporate card. All team members who participate in any of these activities must carry a corporate card or have another team member with a card pay for the event or product.

This completely closes the door to this kind of request. For if you were to reimburse the employee, there could be reportable income ramifications—and nobody wants to get bogged down in that quagmire.

Worst Practice: Making an exception; for once you open the door for one employee, others will demand the same treatment.

Special Pointers for Accounts Payable: You may be tempted to honor the first request you receive like this, figuring it is a one-time occurrence. Alas, you would be wrong. Questionable behavior begets more questionable behavior. The company that first reported this issue said the first occurrence in its shop was six months ago. There were two more requests after that from different individuals. People talk. As discussed above, to avoid getting involved with this, simply update your policy to prohibit it—and if anyone pushes back, remind them there *could be* taxable income consequences.

Review Questions

68. What is the best practice any organization can have regarding cash advances?
    a. Give them to everyone.
    b. Eliminate them.
    c. Give them only to the sales staff.
    d. Give them only to those who request them.

69. Why are unused tickets a problem?
    a. If not tracked, they will go unused and the organization will get no value for their expenditure.
    b. They are not a problem.
    c. Employees often use them to take their spouse along on a business trip.
    d. They take too much effort to track.

70. When an employee leaves the company, which of the following should not be recovered from the employee?
    a. Excess cash advances
    b. The travel card
    c. Their last pay check
    d. The key to the building

71. Which of the following is typically **not** part of a best practice travel reservation policy?
    a. Requiring the employee get the best price taking into account whether the trip might need to be canceled
    b. Ensuring policy compliancy
    c. Ensuring travel begins on a weekend day
    d. Ensuring use of preferred providers, if preferred rates have been negotiated

72. What is the best practice method for reimbursing employees for business travel?
    a. Paper check mailed to the home
    b. Paper check picked up in the accounts payable office
    c. Including expenses in paychecks
    d. ACH deposit separate from payroll

¶1700 Regulatory Issues: Information Reporting

Learning Objectives

Upon completion of this chapter, you will be able to:

Understand what is required for information reporting to the IRS for independent contractors

Develop a policy that will enable the organization to conform with IRS reporting guidelines

Integrate use of IRS TIN Matching into the new vendor setup function

Information reporting in the United States has become a huge issue. Many believe unreported income by small businesses and independent contractors is a large cause for the budget deficit. For some time, legislators and government tax officials have looked for better ways to collect information about all income.

As some reading this might remember, the Patient Protection and Affordable Care Act of 2010 included provisions that would require Form 1099s to be filed for goods and services for everyone starting in 2012. There was much hoopla in the press and lobbying by various special interest groups. This provision was repealed at the end of 2011.

But we shouldn't celebrate too quickly. Virtually every tax professional believes this legislation will be back, probably not in the form in which it was presented earlier but piecemeal in the coming years. Rather than thinking we've dodged a bullet, it would be better if every organization took this as a sign to get their information reporting houses in order. We've been warned and we've got time. In this chapter, we discuss:

A Form W-9/W-8 Requirement Policy
Collecting and Tracking Form W-9 and Form W-8 Policy
Using IRS TIN Matching Properly
Getting B-Notices Despite Using IRS TIN Matching
The Second TIN Match

¶1701 A Form W-9/W-8 Requirement Policy

When vendors are asked to supply a Form W-9 so you can determine whether you have to report their income for tax purposes on the Form 1099, some will balk. They give all sorts of reasons as to why you shouldn't ask for this. They say things like:

If you report my income, I'll have to pay taxes on it.
We don't give this information to anyone.
None of your competitors ask for this.
Please don't report my income.
It's against our company policy to provide this information.

Or, they just flat out refuse to provide it. Some take a more passive approach. They don't refuse, but when you send them a blank W-9 to fill out, they simply don't return it.

At the end of the day, if you don't get this information and report, it is your organization that will be in hot water should the IRS conduct an information audit on your tax reporting. And these audits do happen with regularity. If you are found to be out of compliance, you can be fined. And, if the IRS deems your actions were "willful disregard" of the law, the sanctions can be quite serious.

Best Practice: Require a completed, signed W-9 (or W-8 from your foreign vendors) before the first purchase order is issued. If the vendor refuses to provide it, the order should not be placed. It should also be run through IRS TIN Matching in the case of W-9s as will be discussed later in this chapter.

It should be noted that while W-9s can be provided electronically and are currently good forever or until the vendor has a change in status, W-8s are not. As of early 2013, W-8s are only good for three years and must have an original signature. They are not eligible to be run through IRS TIN Matching either.

Almost Best Practice: If you do not get the completed W-9 before the PO is issued, insist that it be obtained before the first payment is made. That is when you have the most leverage with the vendor. If you wait until after the payment is made, your influence is almost nil, especially if it turns out you will not be doing more business with the vendor in question.

Special Pointers for Accounts Payable: Some of your vendors may point out that it is not a legal requirement that they give you the completed W-9. They are correct. However, you can make it part of your terms and conditions for doing business.

If they refuse to give you the W-9 or the information verbally, you can withhold 28 percent and report and remit it to the IRS. Of course, since you don't have the vendor's TIN, you won't be able to report that and the vendor in question won't get credit for the tax payment. If at all possible, avoid this step. It is messy and cumbersome, will require additional efforts and recordkeeping by your staff, and will likely antagonize the vendor in question. This will not endear you to the purchasing department either.

Worst Practice: Not collecting any taxpayer information at all.

¶1702 Collecting and Tracking Form W-9 and Form W-8 Policy

As mentioned above, asking for a W-9 from a vendor does not guarantee one will be sent. Some simply ignore the issue, hoping it will go away. Others are busy, and sending in the W-9 is one of those matters that falls between the cracks. Since your organization is the one to be fined if correct tax reporting is not completed, it is incumbent on the staff to make sure all the correct information is received.

Best Practices: If you follow the best practice of requiring a W-9 or W-8 before the first PO is issued or at least before the first payment is made, you are well on your way to having the information you need at 1099 time. To be effective, you must:

Send out requests for W-9s,

Track who returned them, and

Follow up with those who have not returned them.

Some are able to do this tracking in their master vendor file; others have to set up a separate mechanism to track. If you have blank fields in your master vendor file, you may be able to set them to categories such as:

W-9 sent to vendor

Completed W-9 received from vendor

W-9 information verified in IRS TIN Matching

By periodically checking these entries, your staff will be able to do the necessary follow-up to get missing information or correct data that was rejected by IRS TIN Matching.

It also should be noted that by doing this kind of tracking, you should be in a good position with the IRS should it conduct an information reporting audit on your practices and it finds you are not in compliance in one facet. By showing that you are assiduously collecting W-9s, tracking their receipt, and running the information through IRS TIN Matching, you will be able to demonstrate that you had good intent. This can help when trying to have fines and penalties abated. For this to help with your case, you must have your tracking in place and you should document your practice in your accounts payable policy and procedures manual.

Almost Best Practice: None.

Special Pointers for Accounts Payable: If it seems to you that the accounts payable function is not getting any easier, you are correct.

Worst Practices: Worst practices include:

Not collecting W-9s.

Sending out blank W-9s and not tracking if you ever get them back.

Not keeping your W-9s together in an easily accessible place, in case of audit.

¶1703 Using IRS TIN Matching Properly

The IRS TIN Matching Program is a free service offered by the IRS. It is an online interactive service offered to payers or their authorized agents. IRS program does as its name suggests. It compares the TIN/name combinations provided with information held by the IRS on its tax filing records. Organizations may use it to verify information for income subject to backup withholding and reported on Forms 1099-B, DIV, INT, MISC, OID and/or PATR.

This matching can be done online interactively for up to 25 entries at a time or in a bulk basis for up to 100,000 entries. If the latter is used, the information is returned 24 hours later.

TIN Matching, under no circumstances, should be used as a phishing expedition to try and determine the correct information. If the IRS determines you are phishing, you will be kicked off the system.

The primary benefit of using TIN Matching is a significant reduction in the number of B-Notices. Organizations that start using TIN Matching report the elimination of between 97 percent and 100 percent of all their B-Notices.

Best Practice: All information provided by vendors on a W-9 should be verified using IRS TIN Matching before the first purchase order is given. If there is a mismatch, corrected information should be requested and run through TIN Matching again.

Almost Best Practice: All information provided by vendors on a W-9 should be verified using IRS TIN Matching before the first payment is made. If there is a mismatch, corrected information should be requested and run through TIN Matching again.

Special Pointers for Accounts Payable: There is really no excuse for not using the IRS TIN Matching program. Anecdotal evidence suggests that the most common reason for not using TIN Matching is executive reluctance. This unwillingness stems from the fact that when registering the organization to use TIN Matching, the executive is required to supply his or her social security number as well as AGI (adjusted gross income) from his or her last tax return filed with the IRS.

It is not uncommon to hear executives complain, “I’m not giving them that information.” In reality, they are not giving the IRS any information it does not already have. The IRS only requests this information so it can identify that the individual signing up the company for TIN Matching is who they say they are. It is for identification purposes only.

If for whatever reason, a company still does not wish to register to use IRS TIN Matching, there is another alternative. TIN Matching can be outsourced, and there are a number of service providers who would be happy to take this on for your organization.

A few organizations run all their information through TIN Matching once a year right before it is time to issue 1099s. While this is better than doing nothing, it is not making the most use out of the system. Vendors are not motivated to send corrected information if you are no longer doing business with them. What’s more, some smaller organizations may have gone out of business or moved, leaving no forwarding address. Better to use it throughout the year correcting information as you go along.

The elimination of most, if not all, B-Notices is cause enough to rush right out and register for TIN Matching.

Worst Practice: Not using IRS TIN Matching.

¶1704 Getting B-Notices Despite Using IRS TIN Matching

If you’ve already started using IRS TIN Matching yet you still get a few B-Notices, you may be wondering why. Typically, these occur because the supplier in question had a change in circumstance during the year and neglected to tell you.

Most of the time, this is not due to malice but because it simply never occurred to the supplier to tell you. It may have moved, merged, changed its legal structure, or something else. Sometimes these related adjustments are the only indication a customer has of such a change.

Best Practice: Before submitting your 1099s to the IRS, take the names and TINs and run them through IRS TIN Matching one more time. This will enable you to catch those pesky vendors who had a change in

circumstance but never remembered to tell you. You'll have to adjust your reporting, but you can do it in your own way without alerting the IRS.
Special Pointers for Accounts Payable: There's one more thing you can do to catch those pesky changes. Any time a vendor makes a change (moves, name change, etc.) ask for a new W-9 and run it through IRS TIN Matching. The reason is simply that the change may also include a change in circumstance that will make the current W-9 invalid. The only way to find out is to get the new information and run it through IRS TIN Matching.

¶1705 The Second TIN Match

Many organizations religiously TIN Match as recommended whenever they get a new vendor, yet they still get a few B-Notices. This leaves them scratching their heads as they were under the impression that if they religiously TIN Matched throughout the year, they could eliminate B-Notices. In theory, this is correct. However, it does not take into account the fact that a few suppliers will have a change of circumstance during the year and never think to tell their customers about it.

The change in circumstance might be a merger, an acquisition, or a change in their legal or tax structure that has no impact on their day-to-day operations.
Best Practice: In addition to getting a W-9 and TIN Matching the information on the form, companies are now advised to TIN Match those vendors who will be given a Form 1099. This should be done when you first pull the information together and before you mail your form and send it to the IRS, so as early as possible in January as is feasible. Then if you discover a mismatch, you can fix it before sending the information to the IRS.
Almost Best Practice: Only TIN Matching when the vendor is first set up.
Worst Practice: Not using IRS TIN Matching.
Special Pointers for Accounts Payable: The advantage of doing this second TIN Match is that if a few items come back, you will have time to fix them and will not have to follow the rigid process mandated by the IRS.

Review Questions

73. What is the best practice when it comes to requesting a W-9 for all vendors?
    a. Require a W-9 before the first purchase order is written.
    b. Leave it to the vendor's discretion as to whether it supplies the W-9.
    c. Let vendors provide the information verbally instead of giving the W-9.
    d. Leave it up to the discretion of the processors.

74. When it comes to W-9s, a good collection policy includes all of the following, ***except***:
    a. Sending out requests to all new vendors
    b. Tracking who returns completed W-9s
    c. Making copies of W-9s sent in
    d. Following up with those who don't return W-9s

75. Which of the following is the best reason to use the IRS TIN Matching system?
    a. It is required by the IRS.
    b. It is easy.
    c. It results in a reduction in the number of B-Notices.
    d. You won't have to issue 1099s if you use it.

¶1800 Regulatory Issues: Unclaimed Property

Learning Objectives

Upon completion of this chapter, you will be able to:

Understand the unclaimed property obligations of every organization

Create a policy that will enable the organization to report and remit unclaimed property in all instances

Develop a practice that takes advantage of social media to track down the rightful owners of your organization's unclaimed property before it has to be turned over to the states

Unclaimed property, also referred to as *abandoned property* or *escheat*, is a requirement that any property that is abandoned or unclaimed be turned over to the state. The rules regarding which state gets the property, when it has to be turned over, and a myriad of other details vary from state to state. When it comes to the accounts payable function, uncashed checks are considered abandoned property.

The rationale behind turning unclaimed property over to the states is that they will hold it until the rightful owner steps forward to claim it. That's why the states are putting information about the abandoned property they hold on the Internet. It helps people track down money that is owed to them. However, not all the information is online, and much of the older data remains in paper or microfiche records.

States everywhere are looking for every last nickel they can get their hands on, so unclaimed property audits are viewed as a source of revenue, despite what you may see in the newspapers. Since unclaimed property gets remitted to the state of the last known address of the owner, and if that is not known, the state of incorporation, unclaimed property is very important to the state of Delaware, where it makes up over 10 percent of the annual state budget. And Delaware is not alone.

In this chapter, we look at best practices related to the:

Reporting and Remitting Unclaimed Property

Performing Due Diligence for Unclaimed Property

Using Social Media to Track Rightful Owners of Unclaimed Property

¶1801 Reporting and Remitting Unclaimed Property

Experts estimate that only about one-third of all organizations who should be reporting and remitting unclaimed property actually do so. This massive under-reporting provides the already-cash-strapped states with a golden opportunity. Many rely on third-party audit firms that work on a contingency basis. These firms perform unclaimed property audits for the states, keeping a percentage of what they recover.

These audits can go back to the date of the last closed audit. If you've never had one, that means they can go back to the day your company opened its doors. But most states are not that cruel. They limit their lookback period to 20 or 30 years. Now, if you are thinking that you don't have records going back that far, you are in for another rude surprise.

If you don't have records for them to audit, the states will gladly estimate what you owe. This is not apt to turn out well for you, so you'll have to hire your own statistician to do an estimate and then negotiate a settlement. You'll not only have to pay what is owed, you'll also owe interest. This can turn out to be a serious amount of money.

Now those reading this may be scratching their head wondering how the state will be able to return the unclaimed property to its rightful owner if an estimate is made on what is owed. How would either party know who the rightful owner was? That is a cogent point. Money turned over as the result of an estimation process cannot be associated with an owner. Hence, it can never be recovered and will remain forever in the state's coffers.

Best Practice: Report and remit your unclaimed property to the appropriate state at the appropriate time. Conduct your due diligence as described later in this chapter.

Almost Best Practice: However, if you are not currently reporting, don't just start reporting. Get an expert to help you. The states will pick up on the fact that it is your first time reporting and an auditor will show up to look through your back records.
Special Pointers for Accounts Payable: The states have claimed that they will audit every organization that falls within their reporting scope. Not reporting and remitting is only putting off the inevitable.

However, if you are not currently reporting, don't just start reporting. Get an expert to help you. Many of the states have voluntary disclosure initiatives, and the expert will negotiate on your behalf, trying to get the penalties and interest reduced. Periodically, some of the states will run amnesty programs. Again, get an expert to help you. These unchartered waters are choppy, and the money you pay the expert to get you in compliance will be well worth it.

There is an ugly practice that occurs in the unclaimed property arena. A third-party auditor will contact your firm offering to get your company in compliance at no cost. Don't be fooled by this offer. The auditor is in all likelihood working for the state and will be paid a percentage of what is recovered during your audit. They will not operate in your best interest nor will they do the necessary research to disqualify items that are really not unclaimed property. Unfortunately, they will probably be back this time wearing their official state hat. So, be prepared to hire your own expert.

There are two additional, somewhat distressing, trends emerging in the compliance arena. The first is that some of the third-party auditors work for multiple states. They may perform audits for all at the same time or come back a second or third time.

The second issue relates to the states' need for money. Some of their own auditors now handle multiple issues. So, for example, the state may send in an auditor to do an information reporting audit and he or she may poke around to also determine if an income tax or unclaimed property audit might bring in additional revenue.

Get all your ducks in a row. Do what you are supposed to do and this will not be a problem.
Worst Practices: Worst practices include:

Claiming your own abandoned property when you are not reporting.

Writing off uncashed checks to miscellaneous income.

Not reporting and remitting your organization's unclaimed property.

¶1802 Performing Due Diligence for Unclaimed Property

The states really don't want you turning over funds to them that will immediately be claimed by its rightful owner. They expect the holder of the funds to do some due diligence to try and find the rightful owner, before turning funds over.
Best Practice: The sooner you follow up on uncashed checks, the easier your work is likely to be. Many organizations follow up at the six-month mark, but 90 days is probably a better option. Send a registered letter with a self-addressed, stamped envelope inquiring about the payment. Save all the documentation. This includes the notification of the registered letter, any returned mail, and the response from the payee. This is important if you decide a payment is a duplicate and reverse it. It is also important if you write the amount off to miscellaneous income. If you can't provide the documentation, the auditor is likely to decide it should be turned over as abandoned property.
Almost Best Practice: If you don't follow up at 90 days, do so at the six-month mark, as described above.
Special Pointers for Accounts Payable: Note that one way to eliminate uncashed checks is to minimize, if not eliminate, checks written. The best way to do this is to move your payments to an electronic platform paying through the ACH. If you do have a bad or inactive bank account number, you'll find that out the next day and can take action. If you can move the bulk of your payments away from paper, you'll greatly reduce your unclaimed property exposure and due diligence required efforts. This is an added bonus few take into consideration when evaluating a move to electronic payments.

Also note that most states have a different dormancy period for payroll checks than they do for accounts payable items. Thus, you'll have to send the money in for the payroll checks earlier than the accounts payable items.

Also be aware that some of the states have been changing their dormancy periods, virtually always shortening them. Dormancy periods are the amount of time you must hold the funds before turning them over to the states. This trend is expected to continue. This means you need to regularly check the state's websites or other resources to find out if the dormancy periods have changed.

Worst Practices: Worst practices include:

Sending abandoned property to the state too early or too late.

Not performing the due diligence required.

Some have tried sending the funds early, not wanting to keep track of them for the entire due diligence period, which for accounts payable checks can be several years. The states return the money. They don't want it early and they don't want it late. They simply want it when it is due.

¶1803 Using Social Media to Track Rightful Owners of Unclaimed Property

As you've probably figure out by now, the due diligence efforts described above can be quite paper-intensive and manual, and the price for completing them can add up. In this time of electronic communication spanning continents, surely there has to be some way to harness this technology to reduce manual efforts with regards to unclaimed property.

Best Practice: Use social media sites to try and find rightful owners. This is especially effective when it comes to uncashed payroll checks, which are typically the last check when an employee leaves the organization. Often they don't realize they are owed that money and move without making arrangements.

A number of companies have had great success locating former employees using LinkedIn and Facebook. Once the potential owner of the uncashed check is identified, they are approached online with an inquiry if they were the same person who used to work for the company in question. On LinkedIn this is even easier as most participants list their former employers.

Almost Best Practice: None—yet!

Special Pointers for Accounts Payable: Obviously, some care has to be exercised when approaching folks on social media sites. If you ask, "Are you the John Jones who used to work for ABC company? We've got some money for you," you are going to get a positive response regardless of whether you've got the right person or not By contrast, other individuals may quickly think this is a scam and will not respond entirely.

Also, some companies block social media sites because they don't want employees wasting countless hours socializing when they should be working. If this is the case in your organization, you can either ask that the block be lifted on a particular account or perhaps the research could be done when working remotely.

By using this method for identifying owners of your abandoned property, you save the expense associated with the more manual approach to due diligence. Combine this approach with a move to electronic payments and you'll see the amount of property your organization has to turn over to the state dwindle, hopefully to almost nothing.

Worst Practice: Not exercising proper caution when approaching potential former employees.

Review Questions

76. Which of the following practices will land you in hot water should unclaimed property auditors show up to audit your books?
    a. Reporting and remitting all unclaimed property
    b. Writing off uncashed checks to miscellaneous income
    c. Reporting uncashed checks as unclaimed property
    d. Trying to find the rightful owners of unclaimed property before reporting

77. Organizations are expected by the states to perform which of the following actions regarding their unclaimed property?
    a. Research items to see if they can find the rightful owner (due diligence).
    b. Nothing.
    c. Take classes on unclaimed property.
    d. Study unclaimed property requirements in school.

78. Which of the following is now being used to locate rightful owners of unclaimed property by some organizations?
    a. Twitter
    b. Pinterest
    c. YouTube
    d. Facebook and LinkedIn

¶1900 Regulatory Issues: Other

Learning Objectives

Upon completion of this chapter, you will be able to:

- Construct a policy that includes accruing and reporting use tax for all the organization's sales tax obligations
- Incorporate regular OFAC checking into the payment process to ensure payments are not made to terrorists
- Identify potential situations where a payment may actually be a bribe to a foreign official in conflict with FCPA regulations

The number of regulatory issues that need to be considered when addressing the accounts payable function continues to grow. Typically, we only think of the tax reporting (i.e., Form 1099 issues) when it comes to regulatory matters in accounts payable. But, there are more. In this chapter, we take a look at the following:

Proper Handling of Sales and Use Tax
Regular OFAC Checking
Foreign Corrupt Practices Act (FCPA) Monitoring

¶1901 Proper Handling of Sales and Use Tax

Sales tax is a tax on the retail sale of tangible personal property. Keep in mind that sale tax is only paid on retail sales. It is also charged on certain services. Which services are taxed varies from one taxing locale to the next.

Cynics claim that use tax was created for those situations where the states believe they have the right to charge sales tax but legally can't. Hence, if you normally would have paid sales tax, but the vendor didn't charge it because it does not have nexus in the locale in question, you are required to accrue use tax and pay it at the appropriate time.

Use tax is charged by many (but not all) states on the "privilege of storing." In this case, storage means the purchaser's holding or controlling property brought in from out of state that is not intended for resale. The rules for what is and is not subject to use tax are very complicated and vary from state to state. It is imperative that the AP professionals responsible for sales and use tax learn what their state rules are.

In recent years, with the advent of online retailing, the issue of sales tax has become a hot topic. The states want the revenue from sales tax on online purchases, but the online retailers claim they have no nexus and thus do not have to collect and remit sales tax. The concept of click-through nexus has been introduced, and it appears that ever so slowly the online retailers are losing this battle.

More than a few companies have no formal policies and procedures for the sales and use tax responsibility. An auditor who finds a company in noncompliance is likely to be more sympathetic to a company that has a policy in place than to one that has ignored the issue. The existence of a policy indicates that the company intends to pay its sales and use taxes, even if it does not always do it correctly. The lack of a formal policy implies that the company has no plan to pay. Thus, the existence of a policy is a company's first defense against an aggressive tax collector.

There is one last very good reason to have a policy in place. A growing number of states now conduct multifaceted audits. The auditor who comes in to review your organization's income taxes may also glance at your sales tax procedures and perhaps your unclaimed property reporting. If you are found wanting in any of those secondary areas, he or she will either conduct a full-blown audit of those practices or alert his or her colleagues in the applicable area. The bottom line is that it is getting more and more difficult to skirt regulatory requirements—so don't try.

Best Practice: Incorporate a strong policy of verifying sales tax on invoices and accruing use tax where sales tax was not charged but should have. Regularly, verify rates and other changes.

Almost Best Practice: None; there is no halfway measure. Proper handling of both sales and use tax is something every organization must do.

Special Pointers for Accounts Payable: Realize that sales taxes continually change. With over 7,000 taxing entities in the United States, it's a massive job to keep on top of the changes in rates and the changes in items taxed. And, unfortunately, there is no uniformity in what's taxed from one jurisdiction to the next.

If an invoice doesn't have sales tax included, resist the temptation to add sales tax to an invoice before paying it. Typically, organizations that follow this practice want to follow the law but don't want the hassle of accruing, reporting, and remitting use tax. There are several reasons why this is a bad practice. For starters, you might be wrong in your assessment that sales tax is due. Then you've paid money you really didn't owe.

More often than not, you are correct in your assessment. However, the vendor did not add sales tax to the invoice because it does not have an obligation to report the sales tax in your state as it probably doesn't have nexus. Most importantly, the vendor will not report or remit the tax. When you are audited by a state sales tax auditor, you will be found deficient, and have to pay the tax and any penalties the vendor may choose to accrue. The fact that you paid it to the vendor will be your problem. You will be left to try and recoup it on your own. Paying it to the vendor is just as bad as paying it to the wrong state. The right state will demand its money, and you will be left on your own to try and recoup it from the state you paid the funds to incorrectly.

Worst Practices: Worst practices include:

Ignoring the sales and use tax issues.

Paying all sales tax to one state, instead of paying it to the states where it is owed.

Adding sales tax to a payment for an item you will owe use tax on, counting on the supplier to understand what you did and pay the sales tax appropriately.

Not checking employees' expense reports for items that might be subject to sales and use tax withholding.

Not checking purchases made on p-cards to ensure that the appropriate sales and/or use tax was withheld.

¶1902 Regular OFAC Checking

The OFAC regulations pertain to the making of payments to terrorists and other blocked parties. When this issue is mentioned, more than a few think it doesn't pertain to them because, "of course they wouldn't do business with a terrorist." But, it is not that simple. Terrorists masquerade as normal companies, with innocent-sounding names.

The Office of Foreign Assets Control (OFAC) of the US Department of the Treasury administers and enforces economic and trade sanctions based on US foreign policy and national security goals against targeted foreign countries and regimes, terrorists, international narcotics traffickers, those engaged in activities related to the proliferation of weapons of mass destruction, and other threats to the national security, foreign policy, or economy of the United States.

The Department of the Treasury produces a list of entities that US organizations are not permitted to do business with. This list is regularly updated, sometimes as frequently as several times a day.

Best Practice: Before each payment is made, check the OFAC list to make sure none of your vendors have been added to the OFAC list. Sometimes when this is mentioned, people are a bit taken back. But you are tasked with not paying terrorists. And, since that list is updated very frequently, the only way to make sure you don't make such a payment is to check the list every single time you make a payment.

The list can be downloaded from the Department of Treasury's website. A process can be automated whereby the list is updated right before your check run. Then all payments should be verified against the list. It's not as hard as it might sound at first glance.

Almost Best Practice: Some organizations run their entire master vendor file against the OFAC list once a month. While this might allow a few payments to slip through, it is a huge step in the right direction.

Other organizations check all new vendors against the OFAC list and then never check again. While this is better than doing nothing, it is not really sufficient to be in compliance with the law.

Special Pointers for Accounts Payable: Expect to get many false positives when running your vendors against the list. When you get what looks to be a match, you'll need to do a little investigating. Here's an example. When checking the list for a talk I was giving, I discovered a company on the list called The Bamboo Company. Now, there are many companies with this name in a number of different countries, and most are perfectly honest. That's why you will need to do a little more investigating once you find a potential match.

This is another example of how terrorists use names for their organization that make them sound legitimate. It is also why this type of checking on a regular basis is imperative.

Worst Practice: Completely ignoring this issue.

¶1903 Foreign Corrupt Practices Act (FCPA) Monitoring

A similar, but very different, issue is that of the anti-bribery legislation. While this legislation has been on the books since the late 1970s, it has become a hot issue in recent years. The press has had a field day covering several large cases where well-known companies were found to have violated the FCPA strictures.

The FCPA was originally passed in 1977 and later amended in 1988 and 1998. Specifically, its anti-bribery provisions prohibit the offer or promise to pay bribes to foreign officials, foreign political parties or party officials, as well as candidates for political office. Also covered is the payment or authorization of payment to these parties. The payments are prohibited when the intent is to obtain or retain business or to direct business to a particular person. Also prohibited are indirect payments.

The legislation has one exception. Payments made to facilitate or expedite the performance of "routine governmental action" are permitted. Typically, this covers obtaining permits, licenses, or other official documents qualifying a person to do business in a foreign country; processing government documents such as visas and work orders; providing policy protection, mail pickup and delivery, or scheduling inspections associated with contract performance or transit of goods; providing phone service or power and water supply; loading and unloading cargo or protecting perishable products or commodities from deterioration, and so on.

When most people think of bribery, they think of money as the medium of exchange. But this does not have to be, especially under the FCPA. In fact, the act defines a bribe very broadly as "anything of value." So in addition to money, this might include:

An offer of employment for the recipient or someone designated by the recipient
Discounts
Gifts
Lavish meals and other entertainment (including trips)
Stock
A commission
Property

What's more, the bribe is still a bribe if it is paid through a third party or is a future payment. These considerations make it all the more difficult for accounts payable to ferret out payments that are really bribes. This is another reason why it is important to scrutinize expense reimbursements closely.

Best Practice: The first step is to train the accounts payable staff to look at invoices, expense reports, and any other vehicle related to the making of payments for anything that looks like it might be a bribe. The legislation is very complicated, so it is important that everyone who works with these payments understands what they are looking for.

Some of these payments will appear on an expense report and may slide under the radar unless the staff knows to look for them. Once the staff has identified potential items, they should be brought to the attention of management for further investigation and follow-up, if it is determined that something is amiss. Under no circumstances should the invoice processor discuss a potential questionable item with the person who received the payment, submitted the payment, or approved the payment.

Almost Best Practice: None. This is another one of those issues that has to addressed in full for the organization to be in compliance with the law.

Special Pointers for Accounts Payable: Be aware that many of the items will turn out to be false positives. That's why it is imperative that further investigation be done and, if there is an item that was paid inappropriately, management be involved. This is an extremely delicate matter that if handled incorrectly could result in a lot of trouble for the organization with the Department of Justice. No one wants to go down that road.

Worst Practice: Ignoring the issue completely.

Review Questions

79. Which of the following is ***not*** a worst practice when it comes to proper handling of sales and use tax?
    a. Accruing use tax on items where sales tax was owed but not collected
    b. Paying all sales tax owed to one state
    c. Not checking purchases made with p-cards to ensure the proper sales tax was collected
    d. Adding sales tax to an invoice payment if the vendor forgot to include it

80. When should vendors be checked against the OFAC list from a best practice standpoint?
    a. Once a month
    b. Only when the vendor is set up
    c. Before each payment is made
    d. Annually

81. The Foreign Corrupt Practices Act specifically forbids bribery to which of the following parties?
    a. Anyone
    b. Foreign officials
    C. Foreign vendors
    d. Foreign employees

¶2000 Technology

Learning Objectives

Upon completion of this chapter, you will be able to:

Craft a policy for the receipt of invoices, regardless of the manner in which they are delivered

Create a process to effectively deal with invoices that are e–mailed

Develop a policy to address the emerging issues related to the use mobile devices (smartphones and tablets) in accounts payable

Gone are the days when accounts payable's technology plan consisted of getting the hand-me-down personal computers when other departments upgraded to newer models. Today, even those organizations not on the leading edge recognize the need to equip their accounts payable staff with modern equipment capable of working with intricate programs and secure high-speed Internet access.

In this chapter, we take a look at the following issues:

An Accounts Payable Technology Plan
Handling E-Mailed Invoices
Invoice Automation
Use of Mobile Devices in Accounts Payable
Getting People to Adopt, Not Fight, New Technology

¶2001 An Accounts Payable Technology Plan

Unfortunately, many organizations still have a haphazard approach to technology issues in accounts payable. They have no formal game plan, simply lurching forward with makeshift training as needed. Rather than sitting back and planning to make sure the entire staff has the equipment they need and the training required, they only step in at the last minute, leaving many of their processes limping along less efficient than they could be.

To be fair, the budget allocations necessary to purchase hardware, software, and training are sometimes beyond the control of the accounts payable manager. But this does not mean that he or she cannot make recommendations based on solid explanations and ultimately influence the inclusion of some funds for the needed technology.

What's more, with the development of the Internet, there are some features that do not require funding. Additionally, there are training and other resources that either cost very little or nothing.

Best Practice: Develop a strategic plan that addresses the hardware requirements of the staff. Of course, this cannot be done until a thorough evaluation has been made of software requirements. This includes identifying not only the software in question, but also the cost of upgrades and training, if any. While the accounts payable manager can make recommendations, he or she typically does not have the final say on this issue.

As part of this strategic plan, identify the software that the staff should be able to use and consider whether any training is needed. Too often, expensive software is purchased and then because no training is offered, only a small percentage of its capabilities are ever utilized. In fact sometimes, because of lack of training, employees are not even aware the software sitting on their computers could perform certain tasks that would make them more efficient and effective.

What follows is a short list of software everyone working in accounts payable should be able to use. You probably have additional entries to the list.

Accounting software used by the organization
Word
Excel
Database management, such as Access

PowerPoint (or other presentation software)

In addition, AP staff should know how to:

Write macros

Create pivot tables

Attend online meetings using gotomeeting, webex, and whatever other new products hit the market

Post job listings on LinkedIn

Search for owners of unclaimed property on LinkedIn (and possibly Facebook)

Google has developed its own version of the Microsoft Office programs, and learning these is a nice touch. Since they seem to be very similar to Office, it is not overly difficult.

Don't assume your staff knows these products intimately. Most people, unless they've had some training or are especially adventurous when it comes to technology, only know the basics.

Finally, be aware that technology is anything but a static issue. To put the matter in perspective, consider that Google began as a research project in 1996. The company incorporated in 1998 and only started selling adwords in 2000. Twitter came into being in 2006, YouTube in 2005, and Skype was first released in 2003.

Technology is making huge inroads in our lives, and the accounts payable function is part of that revolution. Therefore, it is critical that everyone be alert to the next big innovation and be ready to learn how to use it and how to integrate it into the work process to make accounts payable more efficient than ever.

Almost Best Practice: Providing training for all these different products can be tricky especially if you are dealing with a limited budget. But that does not have to be a deal breaker. There are free and low-cost webinars, if you look.

Also, don't overlook YouTube, especially if you have a question about a small feature of Excel or one of the other Office products. There are many short videos posted on YouTube explaining how to use various functions. This is also true of accounting issues, accounts payable issues, and other technology questions.

Pointers for Accounts Payable: Many organizations block websites such as Facebook, YouTube, and sometimes even LinkedIn. They do this as a matter of corporate policy, sometimes because employees have spent too much time on these sites involved in non-company activities. If your organization is one of those, you can either:

Talk to management to see if you can have the restrictions lifted at least on one computer explaining why you need access, or

Access the sites from home and handle the needed tasks there.

Worst Practice: Ignoring the technology issue or trying to stick your head in the sand and pretend the rest of the world isn't changing.

¶2002 Handling E-Mailed Invoices

Electronic invoicing, or e-invoicing, means different things to different people. Some folks use the term to refer to automated invoice processing systems, usually run by third parties. But, most take a more inclusive approach and use the term to include invoices e-mailed by the vendor to the customer, usually in the form of a PDF file.

Research by Accounts Payable Now and Tomorrow reveals that the vast majority of companies now receive at least a few invoices by e-mail. This growing practice puts some form of e-invoicing within the reach of virtually every organization.

Best Practice: Develop a policy for encouraging vendors who are not using third-party e-invoicing systems to e-mail their invoices. This benefits not only the supplier but the customer as well. Invoices are received quickly and can be routed for approvals. If the company is using an imaging process, it saves the company the time and expense of having to do the imaging itself.

Establish a routine for handling invoices e-mailed by suppliers. It might include the following:

Set up one e-mail address to receive invoices from suppliers.

Provide this e-mail address to suppliers, either in the Welcome Packet or annual letter to vendors.

Vendors should be informed that only invoices should be sent to this address. Nothing else sent there will be forwarded.
Vendors should be instructed not to send a second invoice by snail mail. Be aware that some will disregard this directive.
The e-mail address should not be an address associated with an individual but rather one that can be access by several people
Different people can be assigned to forward the e-mails in the account on different days and can fill in for each other when someone is out or on vacations
Upon receipt of the invoice, it should immediately be reviewed and forwarded to the appropriate party for approval.

If you have a fax number set up to receive invoices, and you should, connect it to an e-fax facility. This will convert the paper invoice to an e-mail, and you'll never see a piece of paper.

Almost Best Practice: For those who still prefer the paper, and there are more than a few such companies, establish a routine similar to the one described above for handling e-mailed invoices. The reason for this is that some vendors are now refusing to mail invoices, claiming it is too expensive.

Thus, whether an organization wants to or not, it is going to be forced to deal with e-mailed invoices. So, it is best to have a policy. And those who establish a policy for vendors insistent on e-mailing invoices may find that they prefer this method of delivery. When that happens, they will then begin to encourage all vendors to deliver invoices electronically.

Special Pointers for Accounts Payable: With the advent of the PDF invoice, as well as advances made by technology, it is now very easy to have many original-looking invoices. What's more, fewer and fewer suppliers are marking the second invoices they send as *Duplicate* or *Copy*. Hence, we need to change the way we look for duplicate invoices.

What's more, with a sizeable number of suppliers both snail mailing and e-mailing the same invoice, duplicate checking routines have never been more important. Stringent coding standards and standardized routines for processing invoices are important, for it is no longer possible to identify a duplicate or copied invoice simply by looking at it.

Worst Practices: Worst practices include:

Refusing to accept e-mailed invoices.
Not establishing an e-mail address for invoices to be sent.
Allowing the use of employees' e-mail accounts to receive invoices (and when they leave the company those invoices end up nowhere).

¶2003 Invoice Automation

Invoice automation has come a long way in just a few short years. Typically, the process includes an imaging and workflow, although even the imaging portion has decreased as much of the information is delivered electronically. Although some large companies have developed their own proprietary models, most of the invoice automation today is handled by third-party specialists. The price for this service has dropped drastically, and many now offer their services on a pay-as-you-go basis.

Implementation time has also dropped, along with time needed by in-house IT staff. While their involvement is usually required, the amount of time they must devote to getting these invoice automation projects up and running is minimal. Some of these systems can be up and running six to eight weeks after a contract is signed.

Best Practice: Learn as much as you can about the different vendor models available. Wherever possible, attend vendor demos so you can get a good feeling for what is available and what service would work best with your organization's invoices. Then take a look at the pricing. You may be surprised to discover not only that the service provider wants your company's business, but that the cost savings associated with using the service is larger than you think. Organizations that have a good portion of their invoices handled through an automated process are able to free up staffers to work on more value-add projects.

Almost Best Practice: None.

Special Pointers for Accounts Payable: Many of the third-party invoice automation systems handle e-mailed invoices without any difficulty. Others will handle the paper invoices you still receive, without a hitch.
Worst Practice: Ignoring this issue.

¶2004 Use of Mobile Devices in Accounts Payable

Technology has made huge inroads in the consumer market as well as the B2B world. Sometimes the lines between the two blur. This has happened with the advent of smartphones and tablets. Many of these devices are being purchased by individuals rather than businesses.

What's more, more than a few of the individuals who buy these devices, end up using them for work. While that might not seem like a problem, especially for the company who didn't have to pay for them, it could be when the security issues are considered.

Consider the following data from an Accounts Payable Now & Tomorrow survey. Of those surveyed:
74 percent owned smartphones.
79 percent paid for those phones themselves.
58 percent of those who paid for the smartphone themselves, use it to check work e-mail.

When it comes to tablets, the statistics are even more alarming.
50 percent own tablets.
92 percent paid for tablets themselves.
75 percent of those who paid for the tablet themselves, use it to check work e-mail.

While it is a good sign that so many people involved in the accounts payable function are so interested in technology and willing to pay for it out of their own pockets, we can't overlook the security issues, especially given the rise in ACH fraud, most notably corporate account takeovers. Anecdotal evidence from practitioners reveals that some managers are releasing ACH and wires from their smartphones and tablets during meetings. Again, while the efficiency of multitasking is great, the security concerns should not be ignored.
Best Practice: Create a corporate policy regarding the use of personal devices (smartphones and tablets) for company business. If the practice is permitted, then the devices must have anti-fraud and anti-virus software installed and updated on a regular basis. If these devices are to be allowed for company transactions, they should be included in whatever regime is used for all company computers when it comes to security measures.

If the organization does not wish to include these devices in its security measures, a policy should be established prohibiting the use of personal devices for company business.
Almost Best Practice: None.
Special Pointers for Accounts Payable: This is just one example of the rapidly changing technology world and how it affects the accounts payable function. In all likelihood, employees believe they are being helpful when using personal devices for company business. However, they have not thought the issue through.

As time goes on, there will be an increasing number of issues just like this. And, every organization needs to continually evaluate these issues, see if and how they affect their organization, and develop policies to address the new concerns.
Worst Practice: Ignoring this issue.

¶2005 Getting People to Adopt, Not Fight, New Technology

Sometimes even the smartest, most motivated staffers seem to drag their feet when a new technology is introduced. This can be disheartening for those running the accounts payable function for often the decision has been made, the technology purchased, and there is no turning back. Yet, the skeptics and naysayers will continue to dig in their heels resisting the change. This adds to the workload of the already overworked

manager. What's going on? And, more importantly, what can you do to get them on board because, let's face it, if the decision has been made and the money spent, the new technology will be here to stay.

We all know that some people fear change. But is it the technology itself that they fear? Although they may find it uncomfortable to learn and how to use it and adapt, that is frequently not the real problem. The elephant in the room, the unspoken concern, is what change the technology will bring and, most importantly, the negative impact they fear it will have on their job. To put it more bluntly, it is a question of job security.

By understanding this and addressing staffers' fears before they've had a chance to dig their heels in and cause all sorts of trouble, you'll be getting the new technology program off to a strong start.

Best Practices: Let's take a look at a few steps you can take to ensure a successful launch of the new technology in your accounts payable function.

Best Practice #1: Keep everyone in the loop. As soon as it becomes apparent that new technology will be used, start talking about it with the staff. Don't let them hear rumors from other departments or groups. They will always be exaggerated and make the situation worse. This can be an opportunity to build trust and team spirit. Update staff on a regular basis on what's going on and especially if there have been successes in other departments.

Best Practice #2: Address their fears. Ignoring the issue, hoping it will go away, is naïve. The fears won't disappear miraculously, and the longer a staffer has to ponder it and worry, the bigger the fear will become. So, rip the bandage off and address it right from the start. Be honest, even if the truth isn't pretty.

Best Practice #3: Don't forget the WIIFT (what's in it for them) factor. This means pointing out the benefits of the new technology, not for the company but for the end users, especially the staff concerned about losing their jobs. Maybe it means less keying of data and more time to do more value-add tasks. Or maybe it will mean the end of mandatory overtime. Focus on the benefits for them, not the company, when discussing it with the staff.

Best Practice #4: If you are using a phased-in approach, start with your early adopters and influencers. Get them on board first and let them be your missionaries or evangelists, singing the praises of the new technology. This means that the first few folks brought on board might not be your most senior people but rather those who are likely to embrace the change. This may not sit well with your supervisors, especially if they are part of the group resisting the change. Plan on having a chat with them about this.

Best Practice #5: Realize that the training is not likely to be a one-size-fits-all. Some of your staff will grasp the new technology right away, and others will need additional time and effort. Customize the training to meet the individual needs of each staff person. You might have to run a more basic session for those who are not conversant with technology in general and a shorter, quicker session for the tech-savvy of your group. The important issue here is to make sure the training fits the needs of the individuals.

Best Practice #6: As much as possible, make the training and adoption entertaining. Injecting a little fun into the process will make people forget that they want to object. Of course, the fun aspects relate more to the training than the actual job. How can you do that? For starters, try to introduce some aspects of gamification into the training. No one is expecting to play games and have fun when they go for training. So, incorporating game-playing will be a surprise, and hopefully a nice one.

Almost Best Practice #1: Try taking a carrot approach to getting everyone to use the new technology. You can encourage usage by rewarding employees in ways that might be meaningful to them. For some, it might simply be the opportunity to learn something new. But not everyone will fall into that group. Others might want something more material. This might mean time off, less overtime, a staff luncheon, or something that they select.

Almost Best Practice #2: When all else fails, you'll need to take a harsher stance. At some point, perhaps when you've gotten most of the team on board, you'll have to mandate the use of the new technology. Set a target date for 100 percent usage and make sure everyone knows what it is. When that date comes, rip the band-aid off and insist everyone use the new technology. One organization went so far as to remove the old technology from everyone's computer over the weekend before the 100 percent go-live date. At that point, the staff had no choice. Hopefully, you don't have to implement this step.

Not only will this help get the first group to undergo the training on board, it will help in another way. When this group returns, they'll tell their peers what a good time they had at the training and inspire them

to want to adopt the new technology as well. Talk to the technology provider during the purchase phase about what possible gamification training it might have to offer.

Another approach is to set up a competition between different staff members. Or perhaps divide the group into a few small teams and let them compete. This will result in the added benefit of having other team members encourage each other, rather than the manager being the bad guy who is insisting they make the change.

Worst Practice: Ignoring the issue.

Special Pointers for Accounts Payable: There's lots of change coming to the business world and more specifically to the accounts payable function. When it comes to implementing change, functions that contain easily-replicable repetitive steps are at the top of the list for new applications currently being developed.

The invoice processing part of the accounts payable function falls into that group, and it hasn't escaped the notice of the application developers. Expect to see continued automation in that area as well as other accounts payable and accounting functions. This is not the only place to expect change, although it is likely to be one of the first. By using the steps discussed above, you may be able to make the transition a little easier for the staff and smoother for the organization.

Review Questions

82. Which of the following describes a best practice technology plan for the accounts payable function?
    a. It should be rigid and not change too much.
    b. It should be as flexible or rigid as the staff likes.
    c. It should always take advantage of the newest innovations.
    d. It should be flexible to adapt to whatever new innovations are developed.

83. Invoices accepted by e-mail should all be sent to which of the following?
    a. One centralized e-mail address used specifically for this purpose
    b. The purchasing person responsible for the transaction
    c. The accounts payable managers personal e-mail address
    d. Wherever the vendor wishes to send them

84. Which of the following is a good place to learn about invoice automation?
    a. The newspaper
    b. Popular magazines
    c. Vendor webinars
    d. The radio

85. Why shouldn't employees use their own devices (smartphones or tablets) to release ACH transactions and wires?
    a. The company didn't pay for the devices.
    b. The devices may not have the proper security protections.
    c. The devices aren't capable.
    d. The devices make mistakes.

¶2100 Communications/Vendor Relations

Learning Objectives

Upon completion of this chapter, you will be able to:

Identify methodologies for communicating relevant payment information to vendors before problems arise

Develop a policy for effective communication with internal customers

Cultivate ways to work effectively with the purchasing department

The accounts payable function is an integral part of the finance and accounting chain. To operate efficiently, it also has to communicate regularly with vendors. In this chapter, we investigate best practices related to:

Communicating Relevant Information to Vendors
Communicating with Internal Customers
Working with Purchasing
Customer Service in Accounts Payable
Dealing with Employee Who Do Not Use Approved Vendors
Dealing with Critical Vendors

¶2101 Communicating Relevant Information to Vendors

While payment and invoice status information is important to vendors, it is not the only information needed by vendors. If the vendors are not educated in the beginning about what they need to do to get paid, the payment process is likely to be rocky—especially from the vendors' point of view. Similarly, when a payment is sent, if it is not for the exact amount of the invoice, the vendor is likely to have questions. And, those questions will result in numerous phone calls to accounts payable. This leads to poor vendor relations and inefficiencies in the accounts payable department. Hence, anything that can be done to improve the information flow to vendors not only improves vendor relations, but also the efficiency of the department.

Best Practice: From the day the relationship starts, vendors must have all the information they need about your processes, procedures, and requirements. This can be done utilizing one or more of the following vehicles:

A welcome letter spelling out your requirements, such as
- Where invoices should be sent,
- Special terms,
- Bill-to address, and
- Other special requirements.

A handbook detailing requirements for payment. This can be quite detailed, as is the case with some of the bigger retailers.

A spot on the website that spells out the information that is included in the manual or in the welcome letter. This allows the vendor to know what it is getting into before the fact.

The other piece of information that vendors require is a list of:

The accounts payable contacts,
These individuals' phone numbers, and
Their e-mail addresses.

Depending on how you handle vendor inquiries, this can be the same person who processes vendor invoices or someone who does nothing but address vendor questions.

While this may seem obvious, it is one of the issues that vendors repeatedly bring up when asked about when discussing relations with their customers. Needless to say, this information should be updated and shared with vendors whenever there is a change.

Letting the vendor know what is expected, is only the first step. As discussed previously, providing a self-service function that allows vendors to check on payment and invoice status is another best practice, especially if dispute resolution can be incorporated into that process.

The other area that can be improved relatively easily is the sharing of information with vendors when anything other than the full amount is paid on an invoice. Make no mistake about it, sharing the information will not end the phone calls, but it will reduce the number of phone calls needed to resolve issues. Most deductions taken by companies will fall into several broad categories. While some of the deductions—including early payment discounts, damaged goods, short shipments, and penalties—might be commonplace, others will be unique to the company or industry. Prepare a simple form that can be included with the payment. If at all possible, have this information printed on the remittance advice part of the check. If you are paying electronically, send this information along in an e-mail to the person handling cash application at your vendor.

When the vendor receives the data, it may still call. But the call asking the reason for the deduction and the ensuing research will be eliminated.

Almost Best Practice: If the company cannot share information about short payments easily, the accounts payable staff should make some simple notes detailing the reasons for the deductions. Then, when the inevitable phone calls do come, the staff can refer to the notes and easily respond to the inquiry. Given the nature of technology today, this data should be kept in a shared database, so everyone has access to it and can respond to calls on a timely basis.

Special Pointers for Accounts Payable: Calls about payments from vendors will continue regardless of what best practices are instituted by accounts payable. However, the number of these phone calls can be reduced greatly by some of these customer service initiatives. If, for example, the payment status information is available on the Internet, take the time to walk the vendor through checking it, when the vendor calls. Yes, it is quicker to check it yourself. However, the time spent walking the vendor through the process is a good investment, as this vendor will not need to call again.

Worst Practice: Some companies don't share information about deductions with vendors, hoping that the amounts will be so small that the vendor won't call. Sometimes they are correct. But more often than not, the vendor will call, and call numerous times until the issue is resolved. This also leads to frayed vendor relations and could ultimately result in higher prices or a key supplier deciding not to bid when the next request for proposal goes out.

¶2102 Communicating with Internal Customers

Companies whose accounts payable department has a poor image as well as poor relations with other departments can attribute part of the problem to the fact that the rest of the company doesn't really know what accounts payable needs in order to get payments made, as well as key cutoff dates. This is an issue that is easily remedied.

Best Practice: Accounts payable needs to communicate its requirements to others in the company. This can be done by:

Sharing the AP policy and procedures manual
Periodically sending around a short informative AP newsletter
Publishing the names and contact information of the staffers in accounts payable
Publishing the cutoff dates for T&E payments and vendor payments

The accounts payable department should have a few pages on the company's intranet site. The information indicated above should be included on it for all to see. Transparency should be the name of the game. If the AP policy and procedures manual is long, and many are, a shorter synopsis can be included on the website and/or in a memo to the rest of the company. It is unrealistic to expect others to wade through it to find the information they need.

Larger companies might want to assign one or more people to a customer service function and answer questions the rest of the company might have with accounts payable related issues.

As discussed in other parts of this course, the policy and procedures manual should be updated periodically. Perhaps input from other affected areas could be sought the next time the update is done. Those that have input are more likely to conform to the policy than those who don't.

The old adage of walking a mile in someone else's shoes is a good one for accounts payable and other departments. Occasionally, purchasing and accounts payable are at odds. Having representatives from each department work for a day or two in the other department can lead to a greater understanding of the other's problems. This is also a good idea since the two groups need to work closely.

Accounts payable should track errors to find the root cause of problems. With this data, they can identify weak points as well as other departments that may be causing problems. This does not have to be a negative. Let's say that with the error information, it becomes apparent that one purchasing agent is responsible for numerous voided checks. By meeting that agent and reviewing the process, not only can the situation be rectified, but the relationship may be also strengthened.

Whenever a new system is rolled out, representatives from accounts payable should be sent to interact with other departments to ensure that everyone knows how to use it properly.

Almost Best Practice: Send the staff to customer service courses to help them deal with difficult situations, making sure they understand that they are not the customer.

Special Pointers for Accounts Payable: The very nature of the tasks handled in accounts payable make it likely that there will be conflicts from time to time. These can be both with other departments as well as with vendors. The goal should be to handle these sticky situations with finesse and tact. Vendors will sometimes try and get accounts payable to pay them earlier than their contracts stipulate, other employees will occasionally blame accounts payable for late payments they caused, and employees who are tardy about their T&E reports will then try and hurry the process when their credit card bills show up.

By recognizing that these situations will arise and dealing with each separately, relations with internal customers will improve. But don't expect an overnight improvement. It will take time.

Finally, as additional parts of the procure-to-pay function are automated and an electronic audit trail is created, some of the problems will diminish. A lot of the he-said, she-said finger-pointing games will disappear because of the electronic paper trail.

Worst Practices: Worst practices include:

Ignoring the customer service implications of the accounts payable function.

Not working to share information about accounts payable issues with the rest of the company.

Not working with purchasing.

¶2103 Working with Purchasing

Historically speaking, accounts payable and purchasing have not gotten along in some organizations. This does not have to be. In fact, it is better for both organizations if the two can work harmoniously. As accounts payable has become more integrated into the finance and accounting chain, the sometimes-frayed relationship between the accounts payable and purchasing departments has improved.

What's more, as the accounting function in general—and the accounts payable function and purchasing function specifically—have become more automated, providing greater visibility into transactions, the relationship tends to improve.

Some organizations, most notably those *not* in manufacturing, have taken to merging the two organizations under one manager. By having both functions report to the same manager, some of the frictions have been eliminated.

Best Practice: When establishing policy or trying to work on a problem, try looking at it from the other side of the table. Too often, accounts payable fully understands its own issues but does not realize the problems purchasing may have. (And of course, the same goes for purchasing sometimes not understanding the issues accounts payable has.)

Looking at the problem from both sides helps both sides work together and craft solutions and procedures that both departments not only can live with, but can benefit from.

The old adage of walking a mile in the other's shoes is applicable to this situation. Wherever possible, have the purchasing staff spend time working in accounts payable and vice versa. Let the purchasing staff process those invoices that are problematic, let them see all the extra work created by last-minute approvals, and most of all, let them go through the rigmarole of issuing a rush check.

Interdepartmental lunches will also help as will monthly (or quarterly) meetings to discuss problems, air out differences, and develop solutions to ongoing problems.

Almost Best Practice: Doing as many of the above as you can, but not all.

Special Pointers for Accounts Payable: Accounts payable often has the information that purchasing can use to negotiate better rates. By working with purchasing, accounts payable can give purchasing staff the information they need to be more successful.

Worst Practice: Letting poor relations with the purchasing department fester.

¶2104 Customer Service in Accounts Payable

Too often when the issue of customer service is mentioned in accounts payable, the first response is, "Hey, we're the customer and we're always right." It is this type of attitude that gets the accounts payable department into hot water with vendors, purchasing, and other departments within the organization.

Accounts payable has a variety of customers. They include:

Vendors looking for information about payments or invoices

Employees looking for information about expense reports

Purchasing professionals looking for information for suppliers

Other employees looking for information accounts payable may have that will help them with their projects or research

Admins looking for information for their bosses

Best Practice: Start by walking a mile in their shoes. Determine the motivation behind their call and what is really driving them. It may not be what your think. For example, an accounts receivable person who calls looking for a late payment not only may be looking for the late payment, but may also be concerned about their bonus, if it is linked to how quickly they collect funds.

Similarly, a small business owner calling looking for a late payment may be distressed because he or she needs that money to meet payroll. By understanding the underlying motivation behind the call, your staff may be more sympathetic.

Make sure you put an employee with good people skills in the position of answering vendor inquiries and other types of questions. Get to know your employees' strengths and weaknesses. This will help you assign the department's work in a manner that matches each employee's key strengths with the tasks that require those abilities. An employee that is very careful and accurate might be a good person to assign data entry tasks, while the gregarious, easygoing processor might be the ideal selection to put on the help desk.

Establish a policy of always responding to an inquiry within 24 or 48 hours, even if it is to only tell the person the matter is still being researched. Don't leave them dangling, thinking no one is addressing their issue.

Almost Best Practice: None.

Special Pointers for Accounts Payable: Periodically check and see how the internal customers view the accounts payable department. This means surveying your customers and asking for feedback. It also signals to your customers that their opinions matter. Just the simple act of doing the survey could improve the department's image with the rest of the company. The intelligence that you get from these surveys can be a real eye-opener. But getting the information is just the first step. Then you need to take a cold, hard look at whatever criticism is given and see if and how the actions that generated the negative feedback can be changed.

Realize that no matter how hard you and your staff try, you will always end up with a few disgruntled customers. Your goal is to try and keep that number to an absolute minimum. Before we close on this issue, there is one more point.

Having a customer service attitude in accounts payable does *not* mean turning into a doormat, doing whatever anyone asks. You still need to stick to your best practices and strong internal controls. Don't start issuing a rush check anytime you are asked or return checks to requisitioners. That might make your customers happy, but it is not good for the overall organization. Your goal should be to meet the needs of your customers while maintaining best practices and strong internal controls.

Worst Practices: Worst practices include:

Ignoring the customer service aspects of the function.

Taking a "we're always right" attitude.

Not looking for ways to meet your customers' needs within the framework of best practices.

¶2105 Dealing with Employees Who Do Not Use Approved Vendors

Many organizations go out of their way to negotiate contracts with certain vendors for items they purchase frequently. The reasons for doing this are many, including reduced price based on volume, control over the quality of the items purchased, and data collection. Yet, despite having shared details about which vendors are to be used, occasionally an order will come in from an employee for a non-approved vendor. Let's take a look at a few steps every organization can take to help ensure this doesn't happen in their organization.

Best Practice #1: Make sure you clearly state in your policy which vendors must be used under what circumstances. This eliminates the excuse of "I didn't know we *had* to use that vendor." Like every other policy, it should be widely shared.

Best Practice #2: When a purchase comes through that does use a preferred vendor, call or e-mail to find out why that vendor wasn't used. Sometimes there is a reasonable explanation. Maybe the preferred vendor was out of stock, there was a rush order that the preferred vendor couldn't fulfill, or something else. Of course, the purchasing manager should have been notified. If this is a large enough order, this should be documented.

Once you have the explanation, you can decide what to do next. Depending on the dollar amount, you might want to, at a minimum, copy the purchasing manager on the correspondence.

Almost Best Practice: Report the issue to procurement and let them deal with it.

Worst Practice: Ignore the matter. If the employee is playing games and attempting to defraud the organization, this activity will increase.

Special Pointers for Accounts Payable: If the purchase is large enough, a further discussion with the manager of the area might be in order. Why? Occasionally, you could be looking at fraud. The purchaser could be diverting the order to someone who is giving him or her a kickback or other financial incentive. There have been a few instances where the order has been diverted to a company run by a family member or the purchasing individuals themselves.

¶2106 Dealing with Critical Vendors

A critical vendor is one without whom the organization couldn't operate. At the top of the list are the utilities. If the electric company cuts power, the organization quickly grinds to a stop. The manufacturing facility can't operate and the administrative staff can't power up their computers. And as more than one organization has learned the hard way, the utilities have no sense of humor and they don't care who you are. If you don't pay your bills, they cut off service.

Utilities aren't the only critical vendors for many organizations. For some it is the vendor who supplies the lion's share of their raw materials used in manufacturing, and for others it is the vendor who supplies the key component needed for production. It may not cost much, but if it can only be purchased from one or two suppliers, they need to be treated with kid gloves. It is imperative that accounts payable does everything within its power to ensure none of these critical suppliers decide to cut services or stop supplying those key ingredients.

Best Practice #1: The first step in ensuring critical vendors are treated appropriately is simple. You have to know who they are. This is often not as easy as it would appear at first glance. It is not enough for the managers to know them; the staff should also know who they are so there is no snafu on that level.

Best Practice #2: The next step in your process is somewhat obvious. Once you have identified these key players, make sure you get them paid on time. It doesn't matter how the rest of your suppliers are treated, payments to critical vendors must be made on a timely basis. Don't extend payment terms on their invoices. Even if you have a formal program to delay payments, exclude your critical vendors from those programs.
Worst Practice: Not separating out critical vendors when the organization is instituting a policy that is not likely to be popular with vendors. This could be something like arbitrarily extending payment terms.
Special Pointers for Accounts Payable: As with every vendor, the time will come when you have a discrepancy on one of their invoices. We are not suggesting you roll over and pay it. However, you do need to resolve these discrepancies quickly so the invoice can be paid on time, or as close to it as possible. Make resolving discrepancies on their invoices a top priority.

Finally, when dealing with these vendors, regardless of whether it is over a discrepant invoice or some other issue, don't take a hard-line approach with them. The last thing you need is for them to tell you to take your business elsewhere. This probably means these accounts should be given to your most tactful and diplomatic processor.

Before finishing this discussion, there is one related issue. Sometimes when identifying critical vendors, companies neglect to include vendors who are also customers in this group. If they only buy small quantities from you, it is probably not too big a deal. But, if the vendor in question is also one of your largest customers, poor treatment of that vendor could come back to haunt you.

Remember, the vendor-customer will treat you the same as you treat them. So, if you arbitrarily extend payment terms across the board, you may find yourself dealing with an angry accounts receivable person from your own organization. Why? This is because they may turn the tables on you and extend their payment terms to you, making life difficult for your AR staff.

Review Questions

86. Information can effectively be shared with vendors using all of the following, ***except:***
    a. A welcome letter
    b. The annual report
    c. A vendor handbook
    d. A password-protected section of the website devoted to vendor issues

87. All of the following tactics can be used to communicate accounts payable's requirements with the rest of the organization, ***except***:
    a. Sharing the AP Policy and Procedures manual with others
    b. Periodically sending a short AP newsletter
    c. Writing an article for a trade publication
    d. Publishing cut off dates for T&E and vendor payments

88. All of the following tactics are likely to improve relations between purchasing and accounts payable, ***except***:
    a. Looking at conflicts from the others point of view
    b. Spending time performing the others work
    c. Ignoring the problem when the two staff are sniping at each other
    d. Interdepartmental lunches

89. Which of the following is a worst practice when it comes to customer service in accounts payable?
    a. Taking a "we're the customer and always right" approach
    b. Looking for ways to bridge the gap when there are problems
    c. Looking at the problem from the other's perspective
    d. Responding within a reasonable amount of time to all vendor inquiries

¶2200 Cash Flow Management Issues

Learning Objectives

Upon completion of this chapter, you will be able to:

Understand how payment timing can help and hurt the organization

Develop strategies for sharing critical payment status information with vendors

Create procedures to ensure all early payment discounts are earned

Cash flow is the lifeblood of any organization. It is composed of two flows, cash in and cash out. When it comes to cash flow, accounts payable is all about the cash out. In this chapter, we discuss the following issues:

Taking Early Payment Discounts
Payment Timing
Payment Status Information for Vendors

¶2201 Taking Early Payment Discounts

Early payment discounts represent the best investment opportunity any organization has, except perhaps for those in the loan sharking business. Therefore, it is every organization's best interest to identify as many early payment discounts as possible and take them all. One accounts payable manager claims "the only mortal sin in her organization is missing an early payment discount." In a low-interest-rate environment, they are particularly attractive. Of course, as attractive as they are to the customer, they are equally unattractive to the supplier who offers them. So, many suppliers search like crazy to find instances when their customers took early payment discounts but didn't earn them.

Early payment discounts are the concessions vendors sometimes offer their customers in order to entice them to pay early. The most common payment term to incorporate these inducements is 2/10 net 30. It offers customers a 2 percent discount if they pay the invoice within 10 days of receiving the invoice instead of on the 30th day. There are several problems that often arise in connection with the early payment discount.

The first relates to when the clock starts ticking. Usually, the customer and the vendor have a different idea of when the timing starts—the customer believing that the time starts when the invoice hits the accounts payable department, while the vendor starts counting on the date on the invoice. Of course, if you receive invoices electronically, this is a non-issue.

Companies sometimes have a difficult time processing invoices in a timely enough manner to qualify for the early payment discount. Let's face it, 10 days isn't a lot of time if:

The invoice has to be received in accounts payable and logged in;
A copy has to be sent to the appropriate person for approval;
The approver has to review the invoice, approve it, and return it to accounts payable;
The associate in accounts payable has to process the invoice and schedule it for payment; and
The check has to be printed and signed in the appropriate check run, which can be as infrequent as once a week.

Once again, a move to the electronic world solves many of these problems. It also creates an audit trail that makes it difficult for one party to accuse the other of dragging its feet when in fact it was the one who didn't perform as it should.

So, companies sometimes stretch the period and take the discount a few days after the early payment discount period really has ended.

Best Practice: Take all early payment discounts offered. In theory, companies should perform an analysis to determine if it is financially advantageous to pay early and take the discount. However, interest rates are

so low that such an analysis is a waste of time. When rates are higher, the analysis is an absolute requirement. But it has been a long time since such an analysis was required.

To give you a rough idea, 2/10 net 30 translates to a 36 percent rate of return. Even a .5/10 net 30 would translate into a 9 percent rate of return.

Large invoices that involve an early payment discount should be flagged to ensure that they receive priority handling so the discounts are not lost.

Almost Best Practice: None.

Special Pointers for Accounts Payable: Vendors do not appreciate customers who take early payment discounts without paying within the discount period. Some will try and collect the unearned discounts, and others will eventually raise prices to cover this charge.

Still others accrue the unearned discounts and when an open credit shows up on the books will use it to clear out the unearned discount accrual.

Some companies stretch the early payment term for a few days and will take the discount say up until the 15th day. Whatever the policy regarding taking discounts after the discount period has ended should be formalized and in writing. Be aware that just because the company has a policy allowing it to take the discount after the discount period has ended, does not mean the vendor will go along with it.

Worst Practices: Worst practices include:

Not making taking early payment discounts a priority.

Taking all discounts even when payments are made after the discount period and/or after the due date.

¶2202 Payment Timing

Payment timing games are a zero-sum game. For every day the customer gains by paying late, the supplier loses by receiving the payment an equal number of days after the due date. Yet some companies choose to improve their cash flow by stretching their payment dates, usually without the consent of the supplier. Or, if the supplier consents it is because it is an unequal relationship with the customer being the 800-pound gorilla.

While the company stretching the payments may feel they have gained, there are numerous problems associated with this practice. It takes extra work for the payables staff to manage this process, the likelihood that a duplicate payment will be made when the vendor sends a second invoice skyrockets, and it hurts vendor relations.

This is not to say that if a company is having cash flow difficulties, it shouldn't stretch payments. Sometimes it has no other choice. But, unless there are cash flow problems, payment stretching creates problems where none existed.

Best Practice: Pay the right vendor the right amount at the right time. While I wish I had come up with this, it's only fair to give credit where credit is due. This is the mission statement for the accounts payable department at Lowe's Company Inc. Hopefully, many others have emulated this policy or developed similar policies.

Almost Best Practice: None.

Special Pointers for Accounts Payable: If your organization insists on stretching payments, especially for more than a few days, pay special attention to your routines for identifying duplicate invoices. A vendor that is not paid on time will send a second invoice. Rarely are they marked *Copy* or *Duplicate*. And occasionally, they will have a different invoice number. This makes it particularly difficult to weed out the duplicates.

If the organization is stretching payments, it is a really good idea to utilize best practices throughout the rest of your accounts payable operation. This will make it a bit easier to identify the duplicates before a second payment is made. And, as those familiar with the duplicate payment issue know only too well, few vendors return a second payment without being prompted by the payee. This can be a costly endeavor.

Worst Practices: Worst practices include:

Paying early.

Stretching payments when there is no cash flow issue.

¶2203 Payment Status Information for Vendors

One of the problems for accounts payable is the endless phone calls coming into accounts payable from vendors inquiring about the status of their invoices. Most want to know either why they have not been or when they will be paid. Sometimes vendors will call to find out if you've received their invoice and if it has been scheduled for payment.

These calls are disruptive and do not add any value to the payment function. Worse, they require accounts payable to research the particular invoice and return the call. If there were some simple way to share this information with vendors, the number of phone calls coming into accounts payable could be reduced.

While we refer to this issue as payment status, some call it payment visibility.

Best Practice: First, good policies and procedures with regard to the entire invoice-handling process will ensure that not only do payments get made in a timely manner, but also the number of phone calls inquiring about payment status will decline. Paying on time will also help to reduce the number of calls.

Making this information available on the Internet works very well also. Giving vendors a place to check the information regarding payment and invoice status will make a serious dent in the number of phone calls coming into the department. The information can be put on the Internet. With the appropriate user IDs, passwords, and invoice numbers, vendors can check on the status of their invoices and anticipated payments. This functionality is part of some other products being developed for the accounts payable function.

Interactive voice response (IVR) units allow the vendor to call a phone number and in response to several voice prompts get the status of their invoices and the date the check will be cut. This product takes advantage of similar technology to that used by pharmacies that allow you to place orders for prescription refills, but it did not really take off. This was probably due to the advent of the Internet-based applications.

Almost Best Practice: While not the best approach in the world, some companies that have not found a way to institute best practices by trying one or more of the following:

Assign one or more people to the task of answering these calls and researching the invoice status and replying to the vendor with this information.

Limit the time of day when someone in accounts payable will answer vendor inquiries.

Set up an e-mail address to which vendors can send inquiries.

Refuse to respond to those vendors who continually call before the payment date to see if the invoice has been received and that there are no problems.

Special Pointers for Accounts Payable: No matter how good the company's payment practices and information-sharing facilities, the calls will still come. If the company has implemented some of the best practices and a key vendor calls with an invoice inquiry, someone in accounts payable will have to respond. In order to maintain good vendor relations, it is recommended that every company develop a policy of responding to inquires within 24 to 48 hours.

Worst Practices: Worst practices include:

Having whoever answers the phone research the payment or invoice status that the caller has inquired about.

Research and respond to only those invoice inquiries for payments that are more than 30 days past due.

Review Questions

90. From a best practice standpoint, when should your organization take early payment discounts?
    a. Whenever they are offered if you pay within 5 days of the early payment discount date
    b. Whenever they are offered if you pay within 15 days of the early payment discount date
    c. Whenever they are offered regardless of when you pay
    d. Whenever they are offered if you pay within the early payment discount period

91. What is the best practice regarding payment timing?
    a. Pay the right amount at the right time.
    b. Stretch small vendors.
    c. Stretch all vendors for as long as you can.
    d. Stretch all vendors that don't complain.

92. What is the best way to reduce the number of "where's my money?" calls?
    a. Refuse to take the calls.
    b. Pay on time.
    c. Assign one person to handle all calls.
    d. Only take these calls one or two days a week.

Closing Thoughts

It occurs to me as I finish this work that I've identified a far greater number of worst practices than best practices. And perhaps that is a commentary on best practices. A strategic component in running a best-practice accounts payable operation involves avoiding practices that are likely to cause problems. These difficulties could be as a result of weak controls that enabled fraud or regulatory nightmares or as a result of non-compliance with either state or federal regulations.

But avoiding poor practices is only one part of the equation. Best practices have always been evolving, but the speed at which they have been changing in the last few years is truly startling. What this means is that running a best practice operation also means continually evaluating current practices, looking for those opportunities to improve while simultaneously identifying those practices that no longer work. Unfortunately, the practices that make an organization leading-edge today might not suffice just a few years down the road.

Looking into a crystal ball for the next few years, it is likely that regulatory issues will continue to gain hold as states and the federal government continue to try and close the gaps caused by those not complying. It also is likely that Internet-based innovations will continue to play a significant role in the way the accounts payable function evolves. And evolve it will. Accounts payable is no longer a function operating in its own little silo. It is now an integral part of the accounting and finance chain. And, that is a good thing.

Glossary of Terms

ACFE: Association of Certified Fraud Examiners.

ACH: Automated Clearing House.

ACH credit: An electronic payment initiated by the payor.

ACH debit: An electronic payment initiated by the payee.

AI: Artificial Intelligence.

ASAP payment: see *Rush check*.

B-Notice: An annual IRS notification to payers that IRS Forms 1099 have been filed with either missing or incorrect name/TIN combinations.

Cash advance: Amount of money advance to traveling employees to cover expenses.

CEO: Chief Executive Officer.

CFO: Chief Financial Officer.

Corporate procurement card: See *p-card*.

Detailed meal receipt: Receipt that not only shows how much is due for a meal, but also exactly what was ordered.

Duplicate payment: The unintentional second payment of an invoice. One type of erroneous payment and, unfortunately, rarely returned by the vendor unless the customer or its audit firm discover the over payment.

e-Invoice: An electronic invoice either provided through an automated approach or as simple attachment to an e-mail. Some do not consider files attached to e-mail as true electronic invoices.

Early payment discount: Discount offered for early payment. Discount amount and payment terms indicated in the form of x y/net z, where x = the rate and y= the number of days when the payment is due, if discount is taken and z = due date at full amount. The most common is 2/10 net 30, allowing customers to take a 2 percent discount if they pay by the 10^{th} day after the invoice date with the full amount being due 30 days after the invoice date.

FCPA: Foreign Corrupt Practice Act; prohibits the bribing of foreign government officials.

Form 1099: The Form 1099 is used to report different types of taxable income; the most common for the accounts payable groups being Form 1099MISC. This is used to report income paid to independent contractors.

Gift card: Prepaid card that can be used by anyone to purchase goods or meals at the company designated on the card.

Internal controls: The group of policies and procedures implemented within the organization to prevent intentional or unintentional misuse of funds for unauthorized purposes.

Master vendor file: Repository of information regarding vendors needed to make payments. Can include additional vendor information.

MCC: Merchant Category Code.

NACHA: National Automated Clearing House Association.

NAPCP: National Association of Purchasing Card Professionals.

OFAC: Office of Foreign Assets Control. It is a financial intelligence and enforcement agency of the U.S. Treasury Department. Also see *SDN list*.

P-card: A credit card provided by a company for use in transacting company business. Sometimes referred to as corporate procurement card or purchasing card.

Purchase card: See *p-card*.

Packing slip: Sometimes referred to as *receiving documents*, delineates exactly what was delivered in a particular shipment. Used in the three-way match.

PO: Purchase order.

Receiving documents: See *packing slip*.

Rush check: One produced outside the normal check production cycle, usually in response to an emergency request for payment. Occasionally referred to as an *ASAP payment*.

SOX: Sarbanes-Oxley Act.

SDN list: Specially Designated Nationals list. The SDN List is a compilation of entities and individuals that have been targeted under one or more of Treasury's sanctions programs. US companies are prohibited from making payments to any entity on the list.

Segregation of duties: With regards to accounts payable, it is the division of work so that one person does not perform more than one leg of the procure-to-pay function. It is one of the foundation principles of strong internal controls.

Three-way match: Comparison of invoice with purchase order and receiving documents before payment is made. If there is a discrepancy, some investigation is required to eliminate the discrepancy before payment is made.

T&E: Travel and Entertainment.

TIN: Taxpayer Identification Number; for individuals it is their social security number, and for entities it is their employer identification number.

Travel policy: Document which outlines how an employee is to travel on company business, what is allowable and will be reimbursed and what is not. Also addresses timing requirements of when expense reports should be turned in and the process for doing so.

UCC: Uniform Commercial Code.

Vendor master file: See *master vendor file*.

W-9: Its full name is Request for Taxpayer Identification Number and Certification, and it is provided to customers who need to verify certain tax reporting information. Also referred to as Form W-9.

Answers to Review Questions

1. a. ***Incorrect.*** In all likelihood the AP manager will not be promoted as there will be numerous problems.
b. ***Correct.*** **Poor practices frequently result in a second invoice being sent, and occasionally those second invoices get paid.**
c. ***Incorrect.*** In fact, poor practices are likely to make fraud easier to commit.
d. ***Incorrect.*** When best practices are ignored, financial data tends to be less accurate, and therefore financial statements are apt to be less accurate

2. a. ***Correct.*** **Regulatory problems are likely to increase as the needed information is often not collected.**
b. ***Incorrect.*** Regulatory problems are unlikely to decrease as organizations that ignore best practices are likely to ignore some of their regulatory requirements.
c. ***Incorrect.*** Unfortunately, not using best practices tends to make regulatory compliance more difficult and thus the impact is negative.
d. ***Incorrect.*** Unfortunately, not using best practices tends to make regulatory compliance more difficult and thus the impact is negative rather than the opposite.

3. a. ***Correct.*** **Updating the policy whenever a change is made is the recommended approach to having the most accurate manual all the time.**
b. ***Incorrect.*** While reviewing the policy once a year and updating it for all changes made during the year is a good idea, it will not result in an accurate manual for most of the year.
c. ***Incorrect.*** Never reviewing the policy—or believing once it's set, it's good for life—is an absolute worst practice.
d. ***Incorrect.*** Believing you don't need a policy is another worst practice.

4. a. ***Incorrect.*** By giving only the AP manager a copy of the manual, you don't get the full benefit of it.
b. ***Incorrect.*** By giving only supervisors and managers the manual, you don't get the full benefit of having a manual.
c. ***Incorrect.*** While invoice processors certainly need a copy of the manual, others do as well.
d. ***Correct.*** **Anyone who needs to see the manual should have a copy of it or access to it.**

5. a. ***Incorrect.*** Forgetting about staff training and hoping there will be budget for training next year is likely to result in a staff that is not fully trained. What's more, once an organization removes funding for training, it usually takes several years before it is restored.
b. ***Incorrect.*** Making staff training the responsibility of each member of the staff will result in little or no training and a staff that is not prepared to institute best practices on an ongoing basis.
c. ***Incorrect.*** Bringing in an expert and charging each staff member for a portion of their fees is likely to result in chaos and complaining, and is a really bad idea.
d. ***Correct.*** **Assigning topics and encouraging each staff member to find information on the Internet and then sharing their intelligence with the rest of the staff is a great approach, even if there is funding for training. Developing in-house subject matter experts is great not only for the department but to build staff morale.**

6. a. ***Incorrect.*** Letting anyone in the accounting department update the master vendor file can lead to problems.
b. ***Incorrect.*** Letting anyone in purchasing update the master vendor file can lead to problems.
c. ***Correct.*** **Letting only the few people whose job it is to handle master vendor file data is the best way to prevent collusion and have appropriate segregation of duties.**
d. ***Incorrect.*** Letting anyone in accounts payable update the master vendor file can lead to problems.

7. a. ***Incorrect.*** By not having a firm policy regarding when the vendor should be set up, controls are weakened, the demand for rush checks increases, and other problems ensue.
b. ***Correct.*** **By setting up the vendor in the master vendor file before the first purchase order is written, it is possible to ascertain that the vendor is someone you want to do business with and all the controls are in place.**
c. ***Incorrect.*** By not having a firm policy regarding when the vendor should be set up, controls are weakened, the demand for rush checks increases, and other problems ensue.
d. ***Incorrect.*** By waiting until January to set up vendors, all controls are lost and the likelihood is that many duplicate payments will have been made.

8. a. ***Incorrect.*** Ignoring the naming convention issue and having no standards will result in duplicate vendors in the master vendor file.
b. ***Incorrect.*** Allowing creativity when it comes to data entry will result in duplicate vendors in the master vendor file.
c. ***Correct.*** **Using a rigid naming convention is the recommended best practice.**
d. ***Incorrect.*** Not communicating the standard to all affected parties will result in duplicate vendors in the master vendor file.

9. a. ***Incorrect.*** If updates aren't reviewed, the chances of catching a fraudulent vendor set up by an employee decrease.
b. ***Correct.*** **Reviewing updates with this type of regular report practice serves primarily as a deterrent.**
c. ***Incorrect.*** Having updates reviewed by the person who requested them does nothing to prevent phony vendors from being set up.
d. ***Incorrect.*** While having a clerk in accounts payable review the updates is better than nothing, it does not provide the same force as a senior management review.

10. a. ***Incorrect.*** By letting invoices go wherever the supplier chooses to send them, you guarantee they will not always get to accounts payable in a timely manner. Early payment discounts will be lost.
b. ***Correct.*** **By centralizing the receipt of invoices to one postal address, one e-mail address, and one fax number, you stand the best chance of earning as many early payment discounts as possible and making accounts payable more efficient.**
c. ***Incorrect.*** If you insist invoices are received only by postal mail, you will aggravate suppliers and possibly lose a few key ones.
d. ***Incorrect.*** If you insist invoices are received only by e-mail, you will aggravate suppliers and possibly lose a few key ones.

11. a. ***Correct.*** **A delegation of authority from the board of directors for the right to approve invoices is the correct way to do things.**
b. ***Incorrect.*** By relying on practices that evolved for the right to approve invoices, you are setting up the organization for a potential problem.
c. ***Incorrect.*** By relying on what was always done in the past, you are setting up the organization for a potential problem.
d. ***Incorrect.*** In just about every organization, the AP manager does not have the authority to decide who can approve invoices for payment and who cannot.

12. a. ***Incorrect.*** The headquarters address is not needed to process or pay an invoice.
b. ***Incorrect.*** The website address is not needed to process or pay an invoice.
c. ***Correct.*** **Without either a PO number or the name of the purchaser, accounts payable wastes valuable time trying to figure out who ordered goods and who should approve the invoice.**
d. ***Incorrect.*** A tax ID number is not needed to process or pay an invoice.

13. a. ***Incorrect.*** The receiving document is needed for the three-way match.
b. ***Correct.*** **While a W-9 should be collected from all vendors, it is not used in the three-way match.**
c. ***Incorrect.*** The purchase order is needed for the three-way match.
d. ***Incorrect.*** The invoice is needed for the three-way match.

14. a. ***Incorrect.*** Taking an early payment discount is a legitimate reason for paying less than the total amount shown on an invoice.
b. ***Correct.*** **Take a deduction for problems on another invoice is likely to lead to confusion and further complications with the vendor.**
c. ***Incorrect.*** Taking an advertising allowance is a legitimate reason for paying less than the total amount shown on an invoice.
d. ***Incorrect.*** Using an open credit from an earlier transaction is a legitimate reason for paying less than the total amount shown on an invoice.

15. a. ***Incorrect.*** Without someone reviewing the invoice, you will never know if the invoice is fraudulent.
b. ***Correct.*** **While paying small-dollar invoices without knowing who ordered the goods might save time, it is a terrible practice.**
c. ***Incorrect.*** If you pay a fraudulent invoice, you are likely to get more of them, as crooks learn you don't have good review processes.
d. ***Incorrect.*** Your financial statements will be negatively affected if you pay for something never ordered as this money comes right off the bottom line.

16. a. ***Incorrect.*** Using the date as an invoice number can result in numerous invoices with the same invoice number. What's more, if a second invoice is submitted, it will be assigned a different invoice number and be more likely to be paid.
b. ***Incorrect.*** Using a social security number as part of the invoice number is a really poor practice given all the problems with identity theft.
c. ***Incorrect.*** Processing the invoice without an invoice number makes it extremely difficult to identify potential duplicate invoices.
d. ***Correct.*** **Insisting that all invoices have invoice numbers is a recommended best practice.**

17. a. ***Correct.*** **The invoice number will be of little help when categorizing discrepant invoices to determine the root of possible problems.**
b. ***Incorrect.*** Categorizing by purchaser will help you evaluate whether the problem is in purchasing.
c. ***Incorrect.*** Categorizing by vendor will help you evaluate whether the problem is in something your vendors are doing.
d. ***Incorrect.*** Categorizing by processor will help you evaluate whether the problem is with a particular processor.

18. a. ***Incorrect.*** Paying everything by check is an inefficient way to run the accounts payable function.
b. ***Correct.*** **Encouraging vendors to accept electronic payments is the wave of the future and a recommended best practice.**
c. ***Incorrect.*** Always paying by check unless requested otherwise will result in mostly paper checks. More aggressive action is usually called for when it comes to the move to an electronic payment environment.
d. ***Incorrect.*** Refusing to pay by check might be nice in theory, but in reality will not work as some vendors will refuse to work with your organization if you take this stance.

19. a. ***Correct.*** **A log should be kept comparing the number of checks printed with the check numbers used as a control and safeguard.**
b. ***Incorrect.*** Check stock should *not* be kept near the printer despite the fact that is facilitates work. It also facilitates fraud.
c. ***Incorrect.*** Damaged checks should not be thrown away, but kept to prove to auditors they were not used.
d. ***Incorrect.*** Having checks signed as they are printed by the person printing the checks is a direct violation of appropriate segregation of duties.

20. a. ***Incorrect.*** The accounts payable manager does not have the authority to grant this responsibility.
b. ***Incorrect.*** The treasurer does not have the authority to grant this responsibility in most organizations.
c. ***Correct.*** **The Board of the Directors is where the authority to sign should come from.**
d. ***Incorrect.*** With no one in charge, not only will there be no controls, but also fraud is likely to increase.

21. a. ***Incorrect.*** Storing checks in a secure locked location is a recommended best practice.
b. ***Correct.*** **Storing a few emergency checks in a desk drawer is not recommended as someone who is not authorized to have access might take them.**
c. ***Incorrect.*** Limiting access to check stock is a recommended best practice.
d. ***Incorrect.*** Using a strong lock on the door to the closet where checks are stored is a recommended best practice.

22. a. ***Incorrect.*** Taking checks to the mailroom whenever they are ready to go will result in the checks being in the mailroom longer than they need to be, which increases the chances that someone will walk off with a few.
b. ***Incorrect.*** Taking checks to the mailroom first thing in the morning will result in the checks being in the mailroom longer than they need to be, which increases the chances that someone will walk off with a few.
c. ***Correct.*** **Right before mail is taken to the post office is the best time to take the checks to the mailroom as it will result in them being there for the shortest amount of time.**
d. ***Incorrect.*** Unfortunately, the time checks are taken to the mailroom does really matter.

23. a. ***Correct.*** **Refusing to pay anyone electronically is a worst practice. It is also not practical.**
b. ***Incorrect.*** Insisting on paying electronically may not be a best practice, but it is not the worst approach.
c. ***Incorrect.*** Only paying those who request electronic payment electronically is a step in the right direction.
d. ***Incorrect.*** Making all rush payment requests with electronic payments is a very good idea.

24. a. ***Incorrect.*** Sending a mass mailing to all vendors may result in getting more vendors than you can handle that expect to be converted immediately to electronic payments.
b. ***Correct.*** **Developing a systematized approach to converting all vendors is the best practice response.**
c. ***Incorrect.*** Converting only those who ask is a good start.
d. ***Incorrect.*** Insisting all start accepting electronic payments immediately is neither a best practice nor a worst practice.

25. a. ***Incorrect.*** If you start sending payments to the new account without verifying the request, you could end up paying a crook instead of your supplier.
b. ***Incorrect.*** Verifying the request by responding to the e-mail will land you in hot water if the request is from a crook, for they will verify that the information is accurate.
c. ***Incorrect.*** Verifying the request by calling a phone number provided in the e-mail will land you in hot water if the request is from a crook, for they will verify that the information is accurate.
d. ***Correct.*** **Verifying the request by calling a phone number you already have in your files is the best approach.**

26. a. ***Correct.*** **Asking for extended payment terms is not likely to convince someone who doesn't want to accept electronic payments.**
b. ***Incorrect.*** Paying more frequently with electronic payments than with checks might get the attention of vendors strapped for cash.
c. ***Incorrect.*** Explaining the benefits they will accrue due to their acceptance of electronic payments might convince vendors who do not realize all the advantages of electronic payments.
d. ***Incorrect.*** Paying electronically a day or two before paper checks are released might convince vendors strapped for cash.

27. a. ***Incorrect.*** The policy definitely should address who should have a card.
b. ***Incorrect.*** The policy definitely should address where the card can be used.
c. ***Incorrect.*** A best-practice policy always addresses spending limits.
d. ***Correct.*** **The color of the card is not considered a significant issue; most companies simply take whatever card is provided by the issuer without regard to color.**

28. a. ***Incorrect.*** Merchant Category Code blocks are a good way for ensuring purchases are not made at inappropriate locations.
b. ***Incorrect.*** Monthly review of charge card statements is a strong control.
c. ***Correct.*** **Unlimited dollar transactions for cardholders is a weak control and likely to cause problems.**
d. ***Incorrect.*** Strong card cancellation policies are a strong internal control.

29. a. ***Incorrect.*** Making use of the card optional is likely to lead to decreased usage rather than increased usage.
b. ***Incorrect.*** Only giving cards to employees who request them will not increase usage.
c. ***Incorrect.*** Not educating employees on proper use of the card will result in missed opportunities.
d. ***Correct.*** **Increasing the number of merchants in the program will increase usage.**

30. a. ***Incorrect.*** Corporate cards are not like personal cards, and therefore the payment for the bill is not likely to be due 30 days after the receipt of the bill.
b. ***Incorrect.*** The payment for the bill is not likely to be due 20 days after the receipt. It is more likely to be due sooner than that.
c. ***Incorrect.*** The payment for the bill is not likely to be due 10 days after the receipt. A different time frame is more likely.
d. ***Correct.*** **The payment for the bill is likely to be due 7 days after the receipt of the bill.**

31. a. ***Correct.*** **Evaluating your vendors and deciding what payment vehicle would best meet your needs for paying each is the best way to establish a best-practice strategy.**
b. ***Incorrect.*** Letting vendors decide how they'd like to be paid would result in a mish-mash and is not in your organization's best interest.
c. ***Incorrect.*** Letting the purchasing department decide how it would like each vendor to be paid would not be in line with a best-practice result.
d. ***Incorrect.*** Paying everyone using paper checks would lead to a worst-practice environment rather than a best-practice one.

32. a. ***Incorrect.*** Wire transfers are expensive and not appropriate for small-dollar invoices.
b. ***Incorrect.*** Paper checks are expensive, and using them for small-dollar invoices ties up valuable accounts payable resources that should be focused on larger-dollar items.
c. ***Correct.*** **P-cards are the way to go.**
d. ***Incorrect.*** Use of petty cash is considered a worst practice, and controls are weak.

33. a. ***Incorrect.*** Making it difficult to get a rush check will reduce the number of requests.
b. ***Correct.*** **Asking vendors if they are willing to wait for 14 days for their late payments is not likely to do anything other than weaken vendor relations.**
c. ***Incorrect.*** Insisting on paying rush items electronically will eliminate all rush requests from employees looking to deliver checks in person.
d ***Incorrect.*** Identifying the root causes for rush items and working to eliminate them is a recommended best practice.

34. a. ***Correct.*** **The departments usually don't follow the same strict standards used in accounts payable, and this will cause problems.**
b. ***Incorrect.*** The department making payments only once a week is irrelevant.
c. ***Incorrect.*** This is not one of the causes of problems associated with payments made outside accounts payable.
d. ***Incorrect.*** This is incorrect. It would be true only if rigid standards aren't used elsewhere.

35. a. ***Incorrect.*** ACH blocks are an ACH fraud deterrent.
b. ***Correct.*** **Storing checks in a drawer is a poor practice and won't impact ACH fraud.**
c. ***Incorrect.*** ACH filters are an ACH fraud deterrent.
d. ***Incorrect.*** Use of a separate computer for online banking is a recommended best practice for preventing ACH fraud.

36. a. ***Incorrect.*** A good manual can be used as a training guide for new employees.
b. ***Incorrect.*** A good manual can be used as a reference guide for the accounts payable staff.
c. ***Incorrect.*** A good manual can be used as a reference guide for others in the company.
d. ***Correct.*** **No matter how good an accounts payable policy and procedures manual is, it will never function as a training guide for sales.**

37. a. ***Incorrect.*** Long descriptive paragraphs are not conducive to an effective manual.
b. ***Correct.*** **Bulleted lists are conducive to an effective manual.**
c. ***Incorrect.*** Links to descriptions elsewhere on the Internet are not conducive to an effective manual.
d. ***Incorrect.*** An explanation of the organization's personnel policies is not appropriate nor effective in a manual.

38. a. ***Incorrect.*** Never updating it will result in a useless document.
b. ***Incorrect.*** Updating it every two years will give you a manual that is out of date for a good period of time.
c. ***Correct.*** **Updating it every time a change is made is the recommended best practice and will result in a manual that is always accurate.**
d. ***Incorrect.*** Updating it every five years will result in a document that is useless.

39. a. ***Incorrect.*** By giving access only to the accounts payable manager, you don't get the maximum benefit from the manual.
b. ***Incorrect.*** By giving access only to the invoice processors, you don't get the maximum benefit from the manual.
c. ***Incorrect.*** By giving access only to upper management, you don't get the maximum benefit from the manual.
d. ***Correct.*** **By giving access to anyone who might need to reference it, you'll get the maximum value from your manual.**

40. a. ***Incorrect.*** Since duplicate invoices are rarely identified as duplicate or copy, they are difficult to find.
b. ***Correct.*** **If only invoices were sent on different colored paper, they'd be easy to find. Alas, they are not.**
c. ***Incorrect.*** Duplicate invoices look just like original invoices, making them difficult to identify.
d. ***Incorrect.*** You can print 100 copies of a PDF invoice and they all look like originals, making it very hard to tell which was the original.

41. a. ***Incorrect.*** While refusing to accept such calls would eliminate the problem, it is not an acceptable practice.
b. ***Incorrect.*** Directing such calls to purchasing won't work either.
c. ***Correct.*** **Setting up a vendor portal with this information lets vendors get their own information with disrupting the accounts payable department.**
d. ***Incorrect.*** Paying all invoices as soon as you receive them might reduce the number of phone calls, but it is not an acceptable practice for other reasons.

42. a. ***Incorrect.*** Limiting the items that can be paid through petty cash is a good start but not the best practice.
b. ***Correct.*** **Eliminating petty cash completely is the best-practice recommendation.**
c. ***Incorrect.*** Allowing employees to submit anything under $100 for petty cash reimbursements is a really bad idea.
d. ***Incorrect.*** Reimbursing though petty cash at any time of the day is another really bad practice, making accounts payable inefficient.

43. a. ***Incorrect.*** Never is a worst practice.
b. ***Incorrect.*** Annually is better than nothing, but not ideal.
c. ***Correct.*** **Quarterly is the recommended best practice.**
d. ***Incorrect.*** Monthly is overkill.

44. a. ***Correct.*** **Sharing the organization's personnel policy with all processors will not help achieve a best-practice accounts payable processing function.**
b. ***Incorrect.*** Establishing detailed practices for all to use is part of a best-practice approach.
c. ***Incorrect.*** Developing a rigid coding standard for data entry is part of a best-practice approach.
d. ***Incorrect.*** Periodically checking to verify processors are using standards established is part of a best-practice approach.

45. a. ***Incorrect.*** Weak master vendor file controls do not prevent duplicate payments but facilitate their origination.
b. ***Correct.*** **Timely payment of original invoices is one of the best ways to stop a second invoice and hence a duplicate payment.**
c. ***Incorrect.*** A strict vacation policy will neither help nor hurt the prevention of duplicate payments.
d. ***Incorrect.*** Mandatory overtime at year end will neither help nor hurt the prevention of duplicate payments.

46. a. ***Incorrect.*** Allowing them to be as creative as they like will result in chaos.
b. ***Correct.*** **Following rigid standards set by the manager and used by others in the department is the best way to ensure as few problems as possible.**
c. ***Incorrect.*** Using the standards they used at their prior company, even if that organization was known for its best practices, is not a good idea. With everyone doing things differently, problems will increase.
d. ***Incorrect.*** Allowing them to do whatever they like is likely to cause numerous problems.

47. a. ***Incorrect.*** Double-checking payments on high-dollar invoices is a good way to locate strategic duplicates.
b. ***Incorrect.*** Double-checking payments to vendors known to submit duplicate invoices is a smart strategy and a recommended best practice.
c. ***Incorrect.*** Reviewing payments looking for identical dollar amounts is a great way to find duplicates.
d. ***Correct.*** **Reviewing payments looking for early payment discounts is a good idea but will not help with the duplicate payment issue.**

48. a. ***Incorrect.*** Limiting the number of rush checks is a best practice.
b. ***Correct.*** **Issuing a rush check to anyone who requests one is the worst practice and will cause the number of such payments to skyrocket.**
c. ***Incorrect*****.** Making rush payments with ACH instead of paper checks is likely to discourage some employees from requesting rush payments.
d. ***Incorrect.*** Requiring an approval from a senior level executive to issue a rush payment is likely to cause some to reconsider asking for a rush payment.

49. a. ***Correct.*** **Allowing no single person to handle more than one leg of the procure-to-pay function is what segregation of duties means when it pertains to the accounts payable function.**
b. ***Incorrect.*** Segregation of duties is not affected if someone in accounts payable helps out in personnel.
c. ***Incorrect.*** The computer system for accounts payable must *not* be separate from the computer system for the rest of the company in order to produce financial statements and for other accounting purposes.
d. ***Incorrect.*** Whether employees can or cannot access their work computer from home is not a segregation of duties issue.

50. a. ***Incorrect.*** If nothing is done, you will eventually have a systems access nightmare.
b. ***Correct.*** **It should be closed off to prevent a segregation of duties conflict.**
c. ***Incorrect.*** Promotions are definitely an issue. Unfortunately, they are often overlooked.
d. ***Incorrect.*** Expanding the employee's access is not correct as this will exacerbate segregation of duties issues.

51. a. ***Incorrect.*** It is unlikely the controller will be notified, making it difficult for that person to notify anyone else.
b. ***Incorrect.*** It is unlikely the CFO will be notified, making it difficult for him or her to notify anyone else.
c. ***Incorrect.*** It is unlikely the CIO will be notified, making it difficult for that person to notify anyone else.
d. ***Correct.*** **HR (human resources) is in the loop on employee departures and is in the best position to notify accounts payable.**

52. a. ***Incorrect.*** Using a petty cash box is considered a weak control practice as well as a poor practice.
b. ***Incorrect.*** Returning checks to the requisitioner is considered a weak control practice as well as a poor practice.
c. ***Correct.*** **Using positive pay is a strong control practice and definitely not one that is considered weak.**
d. ***Incorrect.*** Allowing an unlimited number of rush checks is considered a weak control practice as well as a poor practice.

53. a. ***Incorrect.*** It is critical that accounts payable keep on top of best practices as such practices directly affect the way their job is done.
b. ***Correct.*** **Investment opportunities, while important, rarely fall under the accounts payable umbrella.**
c. ***Incorrect.*** It is critical that accounts payable keep on top of new frauds as doing so directly affects the way their job is done.
d. ***Incorrect.*** It is critical that accounts payable keep on top of new regulatory requirements for 1099s as such requirements directly affect the way their job is done.

54. a. ***Incorrect.*** If online banking is conducted on any computer, the chances for an account takeover increase.
b. ***Correct.*** **A separate computer used only for online banking is the best way to guard against a fraudulent takeover of your bank account.**
c. ***Incorrect.*** The CFO's computer is likely to be used for web browsing and e-mail, and therefore is at risk for an account takeover.
d. ***Incorrect.*** The accounts payable manager's computer is likely to be used for web browsing and e-mail, and is therefore at risk for an account takeover.

55. a. ***Incorrect.*** Giving it to the person calling will ensure you give it to any crook who happens to be smart enough to call and ask. Thus, it is not a good practice.
b. ***Incorrect.*** Asking the person for their e-mail address and e-mailing it to them will ensure the information might end up in the wrong hands.
c. ***Incorrect.*** Asking the person for their fax number and faxing it to them will ensure the information might end up in the wrong hands.
d. ***Correct.*** **By not giving it out over the phone at all, you improve your chances of not having the information fall into the wrong hands.**

56. a. ***Incorrect.*** Posting all vendor information where everyone can view it will make it easier for crooks looking to defraud your organization.
b. ***Incorrect.*** Not putting it on the Internet is overkill, if there is an alternative.
c. ***Correct.*** **Putting it on the Internet if you have a password-protected portal for your vendors provides the protection your organization needs against fraud while providing your vendors with needed information.**
d. ***Incorrect.*** It does really matter; posting vendor information correctly is definitely an issue.

57. a. *Correct.* Everyone who has anything to do with the payment function should take at least five consecutive days off. If there is any ongoing fraud, it should unravel in that time period.
b. *Incorrect.* No one is wrong; there is always the risk of fraud.
c. *Incorrect.* By only requiring those in management or supervisory positions to take mandatory vacations, you only address part of the issue.
d. *Incorrect.* By only requiring those who process invoices to take mandatory vacations, you only address part of the issue.

58. a. *Incorrect.* If you go ahead and make the change as requested, you will honor fraudulent requests.
b. *Incorrect.* If you call the phone number provided in the e-mail to verify the request, you will honor fraudulent requests.
c. *Incorrect.* If you ignore the request, you won't be addressing the needs of legitimate requests.
d. *Correct.* Calling or e-mailing a contact using information currently on file is the best way to ferret out fraudulent requests while honoring legitimate ones.

59. a. *Incorrect.* It is absolutely incorrect to indicate that the use of positive pay is not a best practice. It is the best defense against check fraud.
b. *Correct.* Using payee name positive pay, if available, is the best choice and the recommended best practice.
c. *Incorrect.* Of course, use of positive pay is not a worst practice.
d. *Incorrect.* To say use of positive pay is neither a good nor a bad practice is incorrect.

60. a. *Incorrect.* There are best practices related to the use of preprinted check stock.
b. *Correct.* Getting rid of preprinted check stock is the best alternative now that laser printing has made the process much safer and more efficient.
c. *Incorrect.* Use of preprinted check stock is ***not*** a best practice.
d. *Incorrect.* Preprinted check stock absolutely needs special storage considerations.

61. a. *Correct.* A secure locked closet is the recommended way to store preprinted check stock.
b. *Incorrect.* Putting check stock in a file cabinet makes it easy for anyone to steal check and use them for purposes not intended.
c. *Incorrect.* Putting check stock in a desk drawer of an unlocked desk makes it easy for a crook to steal.
d. *Incorrect.* Putting check stock near the printer for ease of use might make it operationally more efficient but exponentially increases the risk of check fraud.

62. a. *Incorrect.* Returning checks to requisitioners is a good way to increase the potential for internal check fraud.
b. *Incorrect.* Delivering checks to the mailroom early in the day will increase the time they spend there as well as the potential for someone to snatch a check made out to someone else.
c. *Correct.* Using positive pay is the best way to prevent check fraud.
d. *Incorrect.* Allowing as many rush checks as wanted can increase the chance for check fraud.

63. a. *Incorrect.* If the policy isn't updated, it will become ineffective and useless.
b. *Correct.* The policy should be updated whenever there is a change. For most organizations this will be several times a year.
c. *Incorrect.* Updating the policy whenever the CFO indicates it should be updated might result in the policy never being updated. This is not a good barometer for when it should be updated.
d. *Incorrect.* Whenever there is a change on the board of directors is not relevant. While it is an important event for the organization, it has little impact on the travel policy.

64. a. *Incorrect.* Ignoring policy violations is an extremely poor practice and will result in an increased number of violations.
b. *Incorrect.* Unfortunately, they are an issue at most organizations.
c. *Correct.* Flagging violations for further review is the best approach.
d. *Incorrect.* It is a waste of effort to flag violations if no one reviews them.

65. a. ***Incorrect.*** If 100 percent of all returns are checked, the organization is wasting valuable resources that could be used elsewhere.
b. ***Correct.*** **Spot-checking 5 to 10 percent is the best approach, especially for large organizations**
c. ***Incorrect.*** Only checking the expense reports of sales will result in potential abuse growing in other parts of the organization.
d. ***Incorrect.*** While in an ideal world no checking would be necessary as managers would have already done it, that approach does not work in the environment we live in.

66. a. ***Incorrect.*** $10 is not the correct response.
b. ***Incorrect.*** $25 is not the correct response, although many believe this is the right level.
c. ***Correct.*** **$75 is the correct response, although few organizations have followed the IRS's lead.**
d. ***Incorrect.*** $1 is not the correct response, although many feel this is the best level.

67. a. ***Incorrect.*** It is not an IRS requirement.
b. ***Incorrect.*** It is not required by Sarbanes-Oxley.
c. ***Incorrect.*** Determining if dessert was ordered won't help much with policy compliance issues.
d. ***Correct.*** **Determining if what was ordered conforms to the policy or if there was fraud is the correct response.**

68. a. ***Incorrect.*** Giving them to everyone will result in a massive and unnecessary tracking issue as well as encourage tardiness when submitting reports.
b. ***Correct.*** **Eliminating cash advances is the recommended best practice.**
c. ***Incorrect.*** Giving them only to the sales staff is not a good idea; no one should get them.
d. ***Incorrect.*** Giving them only to those who request them is likely to encourage everyone to ask for advances.

69. a. ***Correct.*** **If not tracked, they will go unused and the organization will get no value for their expenditure is the correct response.**
b. ***Incorrect.*** They are a problem, especially when paper tickets are rarely used.
c. ***Incorrect.*** While a few employees might use them to take their spouses along on a business trip, that does not seem to be a big problem.
d. ***Incorrect.*** They take effort to track, but that is fine given the fact that they represent value for the organization.

70. a. ***Incorrect.*** Excess cash advances should definitely be recovered.
b. ***Incorrect.*** The travel card should definitely be recovered.
c. ***Correct.*** **Their last paycheck belongs to the employee and should *not* be returned to the organization.**
d. ***Incorrect.*** The key to the building should definitely be recovered.

71. a. ***Incorrect.*** Requiring the employee get the best price, taking into account whether the trip might need to be canceled, is part of a best-practice reservation policy.
b. ***Incorrect.*** Ensuring policy compliance is part of a best-practice reservation policy.
c. ***Correct.*** **Ensuring travel begins on a weekend day is not a good idea and is likely to lead to discontent among traveling employees.**
d. ***Incorrect.*** Ensuring use of preferred providers, if preferred rates have been negotiated, is part of a best-practice reservation policy.

72. a. ***Incorrect.*** A paper check mailed to the home is not the best-practice recommendation.
b. ***Incorrect.*** A paper check picked up in the accounts payable office is a worst practice.
c. ***Incorrect.*** Including expenses in paychecks doesn't provide employees who wish their expense reimbursements to go elsewhere with any flexibility. It is not a worst practice by any stretch of the imagination.
d. ***Correct.*** **An ACH deposit, separate from payroll, is the recommended best practice.**

73. a. *Correct.* Requiring a W-9 before the first purchase order is written is the recommended best practice in this area.
b. *Incorrect.* Leaving it to the vendor's discretion as to whether it supplies the W-9 will result in very few W-9s being collected.
c. *Incorrect.* Letting vendors provide the information verbally instead of giving the W-9 will result in errors in the information due to misunderstandings, transpositions, etc.
d. *Incorrect.* Leaving it up to the discretion of the processors will result in very few W-9s being collected.

74. a. *Incorrect.* Sending out requests to all new vendors should be part of a best-practice policy.
b. *Incorrect.* Tracking who returns completed W-9s should be part of a best-practice policy.
c. *Correct.* Making copies of the W-9s sent in is just busywork and adds no value.
d. *Incorrect.* Following up with those who don't return W-9s should be part of a best-practice policy.

75. a. *Incorrect.* It is not required by the IRS, at least at this time.
b. *Incorrect.* Doing something just because it is easy is not a good reason for doing it.
c. *Correct.* A reduction in the number of B-Notices is the best reason to use TIN Matching.
d. *Incorrect.* This statement is absolutely *not* true.

76. a. *Incorrect.* Reporting and remitting all unclaimed property is what you are supposed to do and won't cause any problems.
b. *Correct.* Writing off uncashed checks to miscellaneous income is a huge no-no. In fact, one of the first places auditors look to make sure you are doing what you are supposed to be doing is at your miscellaneous income account.
c. *Incorrect.* Reporting uncashed checks as unclaimed property is what you are supposed to do and won't cause any problems.
d. *Incorrect.* Trying to find the rightful owners of unclaimed property before reporting is what you are supposed to do and won't cause any problems.

77. a. *Correct.* Researching items to see if they can find the rightful owner (due diligence) is what the states want done. They don't want property turned over only to be immediately claimed by the rightful owners.
b. *Incorrect.* Doing nothing is not correct. The states expect you to return the funds rather than turning them over to the states.
c. *Incorrect.* There is currently no requirement that you take classes on unclaimed property.
d. *Incorrect.* There is currently no requirement that you study unclaimed property requirements in school.

78. a. *Incorrect.* Twitter is not appropriate avenue for locating rightful owners of unclaimed property.
b. *Incorrect.* Pinterest is not appropriate method for locating rightful owners of unclaimed property.
c. *Incorrect.* YouTube is not appropriate manner for locating rightful owners of unclaimed property.
d. *Correct.* Interestingly, Facebook and LinkedIn have turned out to be viable avenues for locating rightful owners of unclaimed property.

79. a. *Correct.* Accruing use tax on items where sales tax was owed but not collected is exactly what you are supposed to do, so clearly it is not a worst practice.
b. *Incorrect.* Paying all sales tax owed to one state will get you in trouble with all the states where taxes are owed except the one you paid.
c. *Incorrect.* Not checking purchases made with p-cards to ensure the proper sales tax was collected is likely to result in a few items being missed.
d. *Incorrect.* Adding sales tax to an invoice payment if the vendor forgot to include it will not get the tax paid; it will simply get you a credit with the vendor.

80. a. ***Incorrect.*** Checking vendors once a month, while better than not doing it at all, is not sufficient.
b. ***Incorrect.*** Checking vendors only when they are set up, while better than not checking them at all, is not sufficient.
c. ***Correct.*** **You should check vendors against the list before each payment is made. This is what is expected, although not many organizations meet this directive.**
d. ***Incorrect.*** Checking vendors annually is not sufficient.

81. a. ***Incorrect.*** The act is not that restrictive, and while it might not be good policy, there are people you can bribe without breaking the law.
b. ***Correct.*** **Foreign officials are specifically mentioned in the act.**
c. ***Incorrect.*** Foreign vendors are not mentioned in the act.
d. ***Incorrect.*** Foreign employees are not mentioned in the act.

82. a. ***Incorrect.*** A policy that is rigid and doesn't change much is not likely to service a best-practice organization well.
b. ***Incorrect.*** A policy that is as flexible or rigid as the staff likes is not likely to provide the best direction.
c. ***Incorrect.*** A policy that always takes advantage of the newest innovations is not likely to distinguish between those innovations that are appropriate for the accounts payable function and those that are not.
d. ***Correct.*** **Making the plan flexible to adapt to whatever new innovations are developed is the best practice.**

83. a. ***Correct.*** **They should be sent to one centralized e-mail address used specifically to receive invoices and nothing else.**
b. ***Incorrect.*** The purchasing person responsible for the transaction should not receive invoices as he or she may not forward them in a timely manner.
c. ***Incorrect.*** The accounts payable manager's personal e-mail address should not be used as it will mix invoices with other items and will not be addressed when the manager is out.
d. ***Incorrect.*** Having invoices sent to wherever the vendor wishes to send them is not a great way to centralize the receipt of invoices.

84. a. ***Incorrect.*** The newspaper is unlikely to have useful or accurate information.
b. ***Incorrect.*** Popular magazines are unlikely to have useful or accurate information.
c. ***Correct.*** **Vendor webinars are a great source of information, especially about invoice automation capabilities.**
d. ***Incorrect.*** The radio is unlikely to have useful or accurate information.

85. a. ***Incorrect.*** The fact that the company might not have paid for the devices has no impact on their suitability for payment work.
b. ***Correct.*** **The fact that the devices may not have the proper security protections is a legitimate concern.**
c. ***Incorrect.*** These devices are very capable, and that is why people are starting to use them for this purpose.
d. ***Incorrect.*** The devices don't make mistakes, so this is not a valid consideration.

86. a. ***Incorrect.*** A welcome letter is a good start to sharing information with vendors.
b. ***Correct.*** **The annual report does nothing to share vital information to vendors on topics of interest to them.**
c. ***Incorrect.*** A vendor handbook is a good way to share information with vendors.
d. ***Incorrect.*** A password-protected section of the website devoted to vendor issues is an excellent way to share information with vendors.

87. a. ***Incorrect.*** Sharing the AP Policy and Procedures manual with others is a good way for others to see what they need to do to get paid on time.
b. ***Incorrect.*** Periodically sending a short AP newsletter is a great way to share information with the rest of the company in a short, interesting manner.
c. ***Correct.*** **Writing an article for a trade publication will do little to communicate within your own organization.**
d. ***Incorrect.*** Publishing cutoff dates for T&E and vendor payments is another great way to share relevant information with the rest of the organization.

88. a. ***Incorrect.*** Looking at conflicts from the other's point of view is a good way to improve relations with any group, including purchasing.
b. ***Incorrect.*** Spending time performing the other's work is a nifty way to understand the other side of the coin.
c. ***Correct.*** **Ignoring the problem when the two staffs are sniping at each other will make the relations worse.**
d. ***Incorrect.*** Interdepartmental lunches are a good way to get the two groups talking to each other.

89. a. ***Correct.*** **Taking a "we're the customer and always right" approach is likely to deteriorate a customer service attitude.**
b. ***Incorrect.*** Looking for ways to bridge the gap when there are problems is a good practice, not a bad one.
c. ***Incorrect.*** Looking at the problem from the other's perspective is a good practice, not a bad one.
d. ***Incorrect.*** Responding within a reasonable amount of time to all vendor inquiries is a good practice, not a bad one.

90. a. ***Incorrect.*** While this isn't the worst practice we've ever seen, paying within 5 days of the early payment discount date is not the best practice.
b. ***Incorrect.*** Paying within 15 days of the early payment discount date is starting to push the envelope and is definitely not a best practice.
c. ***Incorrect.*** Taking the discounts whenever they are offered regardless of when you pay is a worst practice, and most vendors will no longer tolerate it.
d. ***Correct.*** **Taking early payment discounts only if you pay within the early payment discount period is not only the recommended best practice, it is also the fair practice.**

91. a. ***Correct.*** **Paying the right amount at the right time is the recommended best practice.**
b. ***Incorrect.*** Stretching small vendors is an abhorrent practice and not recommended at all.
c. ***Incorrect.*** Stretching all vendors for as long as you can is likely to lead to extra work (and expense) along with an increase in duplicate payments.
d. ***Incorrect.*** Stretching all vendors that don't complain is another less-than-desirable practice and should be avoided at all costs.

92. a. ***Incorrect.*** Refusing to take the calls is likely to create havoc as vendors looking for their money will call other people within the organization.
b. ***Correct.*** **Paying on time is the best way to eliminate these calls.**
c. ***Incorrect.*** Assigning one person to handle all calls will not impact the number of calls.
d. ***Incorrect.*** Only taking these calls one or two days a week will not limit the number and is likely to incense vendors.

Index

References are to paragraph (¶) *numbers.*