

Contributors:

Liz Ashey,  
*Sr. Product Manager*

Lynne Herrman,  
*Sr. Product Manager*

Doug Cranston,  
*Product Manager*



## Best Practices for Fraud-Proof Electronic Payments

### Introduction

The 2009 AFP Payments Fraud and Control Survey found that almost 75% of organizations were victims of payment fraud in 2008, and “nine out of ten organizations that experienced attempted or actual payments fraud in 2008 were victims of check fraud.”<sup>1</sup> And because “the frequency of electronic payment fraud contrasts significantly with the nearly universal incidence of attempted or actual check fraud of greater than 90%”<sup>2</sup>, more and more companies are seeking to implement or increase their usage of electronic payment solutions.

But like any payment method, keeping electronic payments and their accompanying information secure requires the application of traditional risk management techniques, including identifying and assessing those risks. Companies that successfully manage risk can avoid fraud and give their trading partners the confidence they need to adopt electronic payments; the more suppliers that adopt electronic payments, the greater the return on investment for the paying company.

This paper is for companies seeking to understand best practices for electronic payment fraud prevention so that they may realize the increased security, cost savings and process efficiencies that accompany payment automation. Automation of payments alone is taking a step toward fraud prevention; other best practices involve creation of and adherence to risk-mitigating processes along the payment process.

Our company’s payment professionals group the best practices for electronic payment security into the following categories:

- Vendor On-Boarding: “Know Your Customer” Considerations
- Transport: Protecting Sensitive Information as It Moves Through the Payment Process
- Procedures and Personnel: The Human Element
- Physical Plant Security: Safeguarding and Ensuring the Integrity of Tools and Technologies

## Vendor On-Boarding

Establishing a relationship with a new vendor requires precise attention to details. Vendor on-boarding is typically the buyer's Accounts Payable department's first exposure to the new entity. On-boarding may also be performed in cooperation with the company's Procurement area. Some common steps to control against risk include:

- Eliminate duplicate vendor master entries; this is a critical step in protecting against duplicate payments. Verify that the vendor is unique in the vendor master file, and that the vendor master correctly reflects the payment type. If you use a third-party solution provider, require that it provide an analysis of your vendor master file.
- Limit the ability to update the vendor master file; users who can update the vendor master file can change how payments are handled. Dual control and its accompanying checks and balances, which are also addressed below in the section on Procedures and Personnel, come into play here. So if one person has the ability to make changes to a vendor record, those changes should not be allowed to take effect until another person has reviewed and approved the changes. Another precautionary measure is to have the system generate notices of changes and send them automatically to others who hold the same level of authority, so that multiple users have visibility to changes a single user makes.
- Validate that all statutory and company requirements are met. This may include checking the vendor against the Office of Foreign Assets Control (OFAC) lists of proscribed individuals and companies. This step will ensure that your company is in compliance with laws designed to combat terrorism and narcotics trafficking. There are also several statutes designed to combat money laundering. Be sure that you are in compliance with these regulations as well.

### ADDITIONAL CONSIDERATIONS REGARDING EXISTING CUSTOMERS

On-boarding is not a one-time event. It comes into play if you institute a new payment type for an existing vendor, or bring a vendor onto a new payment type. For example, ACH payments require a formal written consent from the vendor, as well as information about the vendor's bank account(s).

Whether your electronic payment solution is in-house or through a third party offering, when moving a vendor to a new payment type, be sure that you:

- Tightly control and coordinate the entire process. A casual, offhand attitude opens opportunities for accidents or fraud.
- Obtain the proper documentation from each vendor. For example, you need written authorization to be paid via ACH.
- Verify that the user at the vendor site who agrees to the new payment type and signs the documentation is authorized to enter into binding agreements on behalf of the company. This controls your liability if any disagreements come up about the payment method.
- Design and enforce a process of verifying the bank account information gathered from the vendor. For example, an individual at the vendor site might try to defraud his or her employer by slipping a personal account number onto the payee list. To guard against this, make it a practice to call the bank and verify that each payee account is associated with a bona fide recipient and not with an individual person.
- Make sure that any account number information gathered from the vendor is protected through encryption (see below). Account number fields in AP should be encrypted; they should not be visible in normal browsing of the vendor master.

*The growth in check fraud has far outpaced the growth in electronic payments fraud. Of the organizations that experienced an increased number of fraud attempts during 2008, 82% report more check fraud while only 18% report more consumer credit/debit card fraud and just 14% more ACH fraud.*

*-The 2009 Payments Fraud and Control Survey by AFP*

- Personnel with the authority to gather, verify, and update vendor banking information should be tightly controlled. Those who perform these duties should not also be authorized to initiate and approve payments.
- Be prepared to explain and document to vendors everything you do to protect their sensitive banking information.
- The foregoing steps and recommendations are primarily tactical. But on-boarding also gives you an opportunity to take a step back and incorporate a few strategic measures:
- Examine third-party campaigning solutions, to determine if there are alternatives to running your on-boarding efforts in-house.
- Carefully target the vendors, so that on-boarding effort is expended where the reward for success is the highest. Follow the “80-20 Rule” and concentrate on the minority of high-value, strategic accounts that get majority of the remittances. These suppliers typically number around 20 percent of your accounts payable roster, but receive close to 80 percent of your payments.
- Track the costs and successes of the on-boarding effort. Aggressive on-boarding support can result in the migration of 50 to 70 percent of your supplier payments to ACH within a six-month span. If you rely on ACH payments through bank channels or others that do not provide on-boarding support, the conversion rate generally runs from ten to 15 percent of payments.
- Take the opportunity to perform associated tasks, such as vendor master cleanup.

## Transport: Protecting Sensitive Information with Encryption and Authentication throughout the Payment Process

### ENCRYPTION:

Think of information security not only for when that information is in transit, but also for when and where it is stored. *Encryption* helps keep information secure through mathematical manipulation that renders data unreadable.

First, understand exactly where your e-payment information resides, and how it gets there. Is it safe from hackers? Is it on a Web page? Is it stored in an encrypted database on a secure server? How does it come in to your company? Is it sent in an e-mail form to your computer?

No payment data moving over the Internet or resting in a file should be readable in plain text. It should be encrypted, using industry-standard methods. When gathering account numbers or other sensitive information from vendors, or in exchanging such data with payment system providers, take special care. Either ensure that the information is not sent via email, or be certain that it is encrypted.

Email is a particular challenge to data security. Email is widely used, but encrypted email solutions are still relatively uncommon, and the encryption offered by many programs is weak and easily defeated. But there are payment system providers that offer free secure email services which can safeguard the information that you transmit to them.

As for the systems used for payment processing, either at the business or at the payment processor site, it is critical that the sensitive fields be encrypted. These fields include any that store bank account information, (whether of the business itself, or of the vendors) and social security numbers, which are sometimes used as vendor identifiers or put into Tax ID fields. None of these number fields should be visible in normal browsing of the vendor master, and encryption will ensure that they remain out of sight. The same care should be taken with any remittance data associated with healthcare claims payments to ensure compliance with HIPAA privacy and security regulations.

**Organizations that suffered financial loss as a result of ACH fraud generally did so because they did not follow best practices and/or neglected to execute their own business rules as expeditiously as they should have.**

*-The 2009 Payments Fraud and Control Survey by AFP*

## AUTHENTICATION:

Verifying the identities of persons or other entities requesting access to the payment system is *authentication*.

There are three ways to verify a user, each of which is called a *factor*:

- Something the user knows (like a password or PIN number)
- Something the user has (like a smart card, token or digital certificate)
- Something the user is (like a fingerprint or retina scan).

A typical system or Web site log-on involves the user entering a user ID and a password. This is *single-factor authentication*; users only need something they *know* to log on.

Single-factor authentication is not adequate for systems involved in critical portions of payment processing. They should use *multi-factor authentication* instead. No critical payment function should be compromised if a user's password is lost, and multi-factor authentication helps to make this possible.

Multi-factor authentication uses two or more factors. Two-factor authentication typically requires a person to prove his or her identity with two of the following items: A password or PIN; a smartcard or token; a fingerprint or iris scan; or a digital certificate. It is more secure than a single-factor system because the user needs more than one piece of information to log on.

For example, a system that uses a normal signing process as well as digital certificates would require that the user *know* something (their password) and also that the user *has* something (the digital certificate stored on their computer). A combination of password and digital signature is recommended here.

## ADDITIONAL CONSIDERATIONS:

Automation of the interface between the Accounts Payable system and the company's payments engine will both speed the entire process and lessen the possibility of human error and purposeful manipulation. The alternative could involve inefficient, error-prone and fraud-inviting practices such as downloading one system's information to spreadsheets before entering it manually into the second system.

## PROCEDURES AND PERSONNEL

Tight controls and well-documented policies provide guidance and governance for employees using the payment system and for those who supervise them and review their work.

Much financial fraud is, unfortunately, perpetrated by dishonest or disgruntled insiders. As a rule of thumb, each worker should have just enough system access to get his or her job done.

In addition to encrypting and safeguarding the information entrusted to your organization, you should be concerned about who has access to the information. Dual control, whereby no single individual is responsible for an entire process, is mandatory. Criminal background checks for all employees are always a good idea, but especially for those who may have access to company or customer funds or vital information.

Workers who have access to the system should have their own separate user identifications. Each person's level of access should be a function of his or her authority and responsibilities. The systems involved in payment processing should support the use of tiered approvals, and these approvals should be configured so that no authorized users have the ability to initial a payment by themselves.

**47% of organizations that were victims of at least one check fraud attempt suffered financial loss as a result, compared to 17% for organizations that were victims of an ACH fraud attempt.**

*-The 2009 Payments Fraud and Control Survey by AFP*

For those who have payment approval or initiation privileges, a separate digital certificate, used to “sign” payments, should be mandated as a second means of authentication. This certificate should be accessible only by the user’s confidential certificate password, and stored in a secure directory.

A secure token is another acceptable option as a second authentication factor. Cost may become an issue with tokens, though, as many banks charge for tokens while digital certificates are frequently free for the end user.

Specific recommendations here include:

- Passwords themselves should be “strong,” with a minimum of eight characters and including one non-alpha character. Tight controls and supervision of passwords is essential. The passwords should be re-set regularly, on intervals not exceeding two months (or shorter, if necessary).
- Second or third digital signatures should be required prior to processing payments. One or more additional approvals can be designated for payments above a certain dollar threshold or to a particular class or type of payee.
- System users who perform maintenance of company, account, and user profile information should have separate and distinct sets of authorities and privileges from those who approve payments. As noted above in the section on Vendor On-Boarding, changes to account information should be made by one person and approved by another individual.
- Databases and accounts, and the user authorities accompanying them, should be segregated appropriately. For example, accounts for employee expense payments, along with their disbursing and approval authorities, should be completely separate from accounts used to pay vendors. In the case of an insurance firm, accounts used to pay claims should be in a separate area of the IT system from employee payroll, investment, and vendor payment accounts.
- Notifications should be built into the system to allow for “checks and balances.” Control emails should be issued to recipients, both inside and outside of the payment workflow stream, whenever payments are issued. These emails also should be generated whenever a sensitive item is altered – such as bank account information or user account privileges. All individuals whose level of authority matches that of the user who made and approved the alterations should be notified; this keeps everyone at that level aware of the actions that any one of their colleagues has taken.
- The system should keep detailed records of log-on, log-off, and timeout events by users. Repeated failures at logging in should trigger a review of the situation and intervention or inquiry from management.
- Managers must not only monitor system access; they should also let employees know their system changes can be tracked. Employers should be wary of people unwilling to share their knowledge about systems or uncomfortable with the fact that their activities accessing systems or data can be tracked.

*The frequency of electronic payment fraud contrasts significantly with the nearly universal incidence of attempted or actual check fraud of greater than 90%.*

*-The 2009 Payments Fraud and Control Survey by AFP*

Audit controls should be built in as well, to allow external auditors and regulators to validate and certify that payments are presented in compliance with all applicable laws and regulations. Reports should be readily available, generated daily, and easy to use so that timely reconciliations of all payments may be performed. The more frequent the reconciliations, the less likely it is that fraudulent payment attempts will go undetected.

## Physical Security and Facilities

Internet-based payment and commerce systems demand multiple layers of physical and virtual protection against hackers, thieves, and potential saboteurs. The servers housing financial information should reside behind multiple firewalls. Only known entities – known and properly on-boarded clients, identified by their IP addresses — should be able to come through the firewalls.

Prudent protection against financial fraud also entails continued testing of systems, including network monitoring and intrusion detection/prevention; and regular penetration testing and vulnerability scanning.

A reliable, off-site backup system for all payment information generated and processed in any given day is a must. Systems should be backed up incrementally at the end of each day, and fully backed up and copied each week. Data centers that process payments should also restrict physical access and segment access by zones. Rigorous control of the space through the use of badges and security cameras is essential as well.

If you use a third-party vendor for your payments solution, be sure to check out the provider's facility. It will give you a good idea of how seriously they take their responsibility to protect your company's important information.

## Summary

If your organization is amongst the 82% that consider increased use of electronic payments for either business-to-consumer or business-to-business payments important for mitigating potential payment fraud risks<sup>3</sup>, the best practices outlined in this paper will help you select a secure solution and establish risk-mitigating processes. Carefully on-boarding and authenticating vendors, ensuring payment information is securely transmitted and stored and establishing employee security measures like checks and balances and activity tracking will empower you and your suppliers to realize the many benefits of electronic payments with peace of mind.

## About Bottomline Technologies

Founded in 1989, Bottomline Technologies is a world leader in collaborative payment, invoice, and document automation solutions for corporations, financial institutions, and banks. Bottomline serves more than 9,000 customers, including 80 of the Fortune 100 companies and 70 of the FTSE (Financial Times 100). Paymode-X™, the largest and fastest growing electronic payment and invoicing network for business, is owned and operated by Bottomline.

To contact Bottomline Technologies about Paymode-X, call or email: 1.800.472.4321

[paymode-x@bottomline.com](mailto:paymode-x@bottomline.com)

## About the Contributors

### DOUG CRANSTON

*Product Manager  
Bottomline Technologies*

Doug Cranston is a Product Manager for Paymode-X at Bottomline Technologies. With an education in computer science, Doug heralds from a technology background and has held various technology positions at Fleet Bank, BankBoston Financial, and Bank of America. Doug subsequently joined the Paymode-X team, working in the Product Management organization. With 10 years of experience working with large corporate and government clients implementing a variety of treasury management services, Doug brings breadth of experience to the Paymode-X team.

### ELIZABETH (LIZ) ASHEY

*Sr. Product Manager  
Bottomline Technologies*

Liz Ashley is part of the Transaction Services NA team responsible for the Paymode-X suite of services. In addition to her Product Management responsibilities she also oversees the strategic development and execution of the Paymode-X Accelerated Enrollment Program, which helps companies to quickly and easily on-board their suppliers. Liz previously managed teams in various business line functions that included Quality Assurance and Customer Service.

Prior to working for Bottomline Technologies, Liz was a Product Manager for Clareon Corporation, where she was a member of the team responsible for the delivery of web-based business-to-business electronic payment and remittance products from concept to market implementation. Liz has over 20 years experience in numerous industries in the area of service improvement, client satisfaction and sales.

### LYNNE S. HERRMAN

*Sr. Product Manager  
Bottomline Technologies*

Lynne Herrman is a Senior Product Manager with Bottomline Technologies, supporting their Paymode-X electronic payment and invoicing network. Lynne joined Bottomline from Bank of America where she also was a senior product manager in their Global Product Solutions division. She has over 25 years of experience working with electronic payments and other treasury management services in both banking operations and product management roles, and has been a periodic speaker at electronic payment conferences. Ms. Herrman holds her B.S. in Economics from Allegheny College and her M.B.A. in Finance from American University. She has earned both Certified Cash Manager and Accredited ACH Professional credentials.

#### Footnotes

1. Association for Financial Professionals, Inc. 2009 Payments Fraud and Control Survey.March 2009.
2. Association for Financial Professionals, Inc. 2009 Payments Fraud and Control Survey.March 2009.
3. Association for Financial Professionals, Inc. 2009 Payments Fraud and Control Survey.March 2009.