Payments

Association for Financial Professionals®
AFP—Your Daily Resource

April 2010

In the April Payments

This month, *Payments* looks at payments fraud, an ever-growing threat. Our lead story examines the growth of payments fraud in 2009, and offers some tips on how to avoid becoming a victim. For this month's Q&A, Bill Nelson, head of the FS-ISAC, talks about a payments fraud exercise for corporates that the information-sharing group organized over three days in early February. Many AFP members participated in the exercise, and should receive best-practice recommendations later this month. Also, Michael Griffith, AFP's legislative analyst, writes an update on cybersecurity legislation.

Cyber Fraud Threat Ever-Growing

Jonathan Starkey

For cyber fraudsters, 2009 was a banner year. Last year, the Internet Crime Complaint Center—a partnership of the FBI and the National White Collar Crime Center—received nearly 337,000 Internet fraud complaints, a 22 percent increase over 2008, the center said in its annual report. The dollar amount loss from the complaints forwarded to local law enforcement agencies was $559.7 million, an increase of more than 100 percent from the $246.6 million loss reported in 2008.

E-mails using the FBI's name were among the most popular ploys that cyber scam artists used. Credit card fraud and identity takeovers were among the most prolific schemes.

"From a wire standpoint, you don't have significant enough volume. That makes it harder to detect."

Also last month, the FBI issued an alert to businesses, warning of increased incidents of ACH and wire fraud. Since 2009, such alerts have become commonplace as fraudsters have targeted the online banking credentials of vulnerable businesses.

"In 2009, it started really ramping up," said Mike Thomas, a partner in the risk consulting group of consultancy Crowe Horwath, said of the cyber fraud threat. "Most banks are only becoming attuned to it only in the last six months to a year."

Banks are using such methods as dual authentication and token technology to ward off attackers, but many businesses remain at risk of attack. Here is how the attacks occur:

An employee will open a fraudulent e-mail, perhaps purporting to come from the company's financial institution, and click on a link, or open an attachment to the message. The

Continued on page 2

Problem Solved

Tracking Deposits

Stephanie Boylan, CTP

As a national telecommunications retailer, T-Mobile relies on an expanding network of retail outlets throughout the U.S. to sell its products. In 2007 there were concerns that we may have been experiencing higher than normal variances with our store cash deposits. These "over" and "shorts" could, in some measure, be attributed to theft. However, a larger percentage also could be blamed on inaccurate deposit reporting by banks and couriers.

We realized the problem would only grow as T-Mobile expanded beyond its current 1,500 outlets. T-Mobile's treasury department sought a solution which:

- Could track deposits from the stores to the bank
- Was Web-based so that managers could input information directly, improving accuracy
- Did not need IT support
- Would strengthen internal monitoring
- Could easily be implemented and rolled out nationally.

Finding a solution

In 2007, **T-Mobile's Director of Treasury, Monica Zaborac, CCM**, and **Retail Treasury Manager Jonathon Saunders** attended the AFP Annual Conference and found International Financial Services (IFS) of Westminster, Md. IFS offered a Web-based tool, Deposit Tracking System (DTS®), which enables sellers to follow deposits from

Continued on page 3

Cyber Fraud Threat Ever-Growing *continued*

attachment or linked Web site is armed with malicious software that will install itself on the employee's computer. Often, that software will log the employee's key strokes, eventually obtaining valuable information such as online banking passwords. Money is then be funneled out using fraudulent ACH transactions and wires and the employee's information. Experts say small and medium-sized businesses, those without complex security walls in place at very large organizations, are at the highest risk.

Wes Wilhelm, a fraud analyst at Boston-based Aite group, said wire fraud can be most tricky to track, because generally there is not as thorough a history on wire account activity as there is in a debit account or ACH transactions.

"The normal use of a debit card, that frequency allows us to distinguish what's good from what's bad—from a wire standpoint, you don't have significant enough volume. That makes it harder to detect," said Wilhelm, who has taught advanced fraud analysis at Utica College.

Wilhelm said the frequency of a particular transaction, how many times a company made a payment to a particular merchant, and the amount of money in a transaction are factors used to build "predictive models" meant to weed out fraudulent payments.

Tips to fight payments fraud

Businesses can take several steps to reduce risk of being a victim of a fraud payments scheme. Wilhelm, Thomas and the FBI (in its annual report) suggest that all businesses take these precautionary measures:

- **Never link to your bank's Web site**. Always type the address into the browser.
- **Immediately report suspicious activity** in your accounts.
- **Be suspicious of e-mails that claim to come from your bank**. Financial institutions should not use e-mail to ask you to verify information
- **Know exactly what your bank's Web site looks like** and what questions are asked to verify your identity. Some cyber attacks will change the login page, allowing the attacker to see your answers to security questions.
- **Dedicate a single computer for online banking access**. The fewer computers that have important information, the less likely it is that the information will be compromised.
- **Consider blocking plug-ins and pop-ups** on computers used for online banking.
- **Use dual authentication and token technology**, so even if your password is compromised, attackers cannot access your accounts.
- **Make sure your bankers know what normal activity in your account looks like**, so they can more easily spot suspicious activity. ▲

Coming Up in Payments

Thanks for reading this month's issue on payments fraud. Over the next few months, we are planning stories on payroll cards—including corporate treasury professionals working to implement paperless payrolls—and how the latest treasury workstation technology can streamline payments processes. Later this summer, Payments looks at check float.

Please feel free anytime to pass along payments coverage ideas, compliments or criticisms to Ira Apfel, AFP's Editorial Manager, at **iapfel@afponline.org**. As always, your input is invaluable.

For advertising opportunities, contact our sales team at **301. 961-8826**.

Payments

Published by the Association for Financial Professionals, Inc.

Editor
Jonathan Starkey

Director, Payments
David Bellinger, CTP

President and CEO
James A. Kaitz

Managing Director, Communications
Elizabeth Johns

Editorial Manager
Ira Apfel

Publications Specialist
Amy Cooley

Payments Editorial Advisory Board
Tom Burrow
Treasury Expert

Anne Marie Gill
Jacques Whitford

Gary Kawka, CTP
Cytec Industries Inc.

Colin Kerr, CTP
Microsoft Corp.

Delores Ratliff, CTP
Target Corporation

Rossana Salaris
The Clearing House Payments Company

Advertising
Advertise in Payments to reach out to decision makers seeking new payments technology. To reserve space today, contact the AFP Sales Team at 301.961.8833.

Subscriptions
www.AFPonline.org/newsletters

Association for Financial Professionals
4520 East-West Highway, Suite 750
Bethesda, MD 20814

Phone: 301.907.2862

Website: www.AFPonline.org

Email: AFP@AFPonline.org

Blog: http://blogs.afponline.org/Payments/

Twitter: http://twitter.com/afponline

LinkedIn: http://www.linkedin.com/companies/association-for-financial-professionals

Join the Distribution List
Each month, Payments will bring you timely news on payments. Sign up today at http:www.AFPonline.org/afppayments.

Newsletter Archive
http://www.AFPonline.org/newsletterarchive

Tracking Debts continued

the stores where they are prepared, to the pickup by armored couriers, arrival at the bank and posting into their account.

The DTS system establishes unique logins for each store and allows area or headquarters managers to access information instantly, indicating whether critical activities have been completed for each store (like whether a deposit has been created, courier has picked up a daily deposit on time, bank adjustments, over/shorts, etc). The DTS system also provides an exception management tool so that when issues occur, automated alerts and reports notify store managers and other key personnel of these problems. All issues can then be collaboratively managed and worked through to resolution.

After reviewing IFS's tool, we believed DTS would decrease the over/short variances T-Mobile was experiencing.

Planning the Implementation

To ensure a smooth roll-out, we enlisted the Retail Operations, Loss Prevention and Sales Audit functional groups. Retail Operations was critical because it serves as the conduit for all communications from Corporate to the field. (We also wanted the Market Managers and Division Directors to help win over the store managers.) Loss Prevention would benefit because DTS would reduce the over/short variances as well as the number of incident reports. Sales Audit was included because the tool would allow it to determine more easily (and quickly) when deposits had not been made and to clean up the exception items list generated by their reconciliation product.

Fortunately, many of the larger banks already use DTS. Thus, the integration of these partners was relatively straightforward. Our initial pilot included a handful of stores across multiple banking partners in 2008. We expanded to 29 stores in early 2009 and started a system wide rollout in March that was completed in June 2009.

With DTS in place, we saw impressive year-over-year (YOY) results when comparing July-December 2008 to July-December 2009. Losses due to cash shortages had dropped an average of 63 percent—despite simultaneously adding 37 percent more stores over that same period. Improved monitoring brought us other benefits, too, like the ability to track armored car pickups.

As noted, we initially used only the largest banks already set up with DTS®. We believed it might not be time/cost effective to integrate the smaller institutions which hold 6 percent of our total store deposits. However, we now expect to bring 79 percent these other banks onboard this year. Additionally, on January 20, 2010, T-Mobile and IFS integrated new system functionality allowing Point-of-Sale information to be directly uploaded into DTS®, eliminating manual entry and further reducing variances.

Final advice

Unquestionably, T-Mobile's savings, through a decrease in over/short variances, have been substantial. As noted, most large banks use the system, but retailers that wish to adopt it should double-check with their partners to determine if all of the vaults being used (including those outsourced) support it. T-Mobile ended up moving over 350 stores to different core banks that had already integrated DTS. However, because of the effectiveness of this new tool, we expect even more of the smaller banks to adopt the system as they learn more about it. ▲

Stephanie Boylan, CTP, is Treasury Manager—Retail for T-Mobile.

Solved a Problem? Tell *Payments*

If your corporate treasury team solved a **payments-** or **risk-related problem** and would like to pass on your advice and lessons learned to your peers, feel free to contact Ira Apfel, AFP Editorial Manager, at iapfel@afponline.org

Your Colleagues Discuss Check Hold Times

Ira Apfel

Recently on AFP's discussion board corporate treasury and finance professionals discussed the challenge of check hold times:

"Our company is reviewing our policy on hold times we establish for check deposits. I wanted to see what other firms are using as guidelines?"
—Anonymous

"Two factors that are important to our position are the fact that we use remote deposit capture and the availability schedule we have with our correspondent. With RDC, same day availability, even on large checks, is not unheard of, particularly with regional, or national, banks. If you deposit the image early enough, the bank can sweep the image and process it through to the paying bank in a very short period of time. That does not mean that you will receive ledger credit or availability for it, however.

"That's where your availability schedule comes into play. If your agreement with your bank is 80/20 where you receive 80 percent of deposited funds next day, and the remaining 20 percent on the second day, your hold period should be two days because you will have received full value in that time. If your availability schedule is different, then that's what you should consider.

"If you don't use RDC, it's a different story."
—Fred Butterfield, CTP, AAP, Treasury Manager, Trust Company of America

"Yes, we do use RDC and receive next day credit, but what hold times do you place on the client's account? Receiving credit isn't the same as the check actually clearing, so do you distinguish between what your company can negotiate with banks and what availability the clients receive? My company is in the financial services broker-dealer business, so our clients deposits a check and then buys securities."
—Anonymous

"One of our principal business units involves trading, so I know exactly what you are speaking about. We have the same situation where a client deposits a check and wants to trade the same day. I have had several discussions with the operations group to define the situation and to help them set their service levels.

"We do not make multiple deposits during the day. Our system allows us to queue transactions. One of the first things we did was set our deposit 'time' later in the afternoon so that funds from that days' deposit were not available in the client account for trading purposes that day.

"Another thing we did was to establish dollar amounts for deposits, as they relate to trading. In other words, if a client really wants to trade on a $1MM deposit, that deposit is made by wire transfer, not by check.

"An additional piece of the picture is related to returned items. If a client deposits a check that is returned for any reason, and the funds have been traded, the client is notified and has a very narrow window to replace the funds with a wire transfer. If the funds are not replaced within that time frame, the trades are unwound and the client is responsible for any market losses there might be, which have to be taken care of before another trade can take place.

"All of this is subject to management override when necessary."
—Fred Butterfield

"Fred's comment about returned items hits the nail on the head. There is a limit on the amount of time that a paying bank has to return a check and your bank needs a processing window to notify you. I would investigate this limit and time frame to make the policy."
—Linda Rodezno, CTP

"We receive checks for purchases into mutual funds, similar to the business Fred described. Our version of a 'hold' on money received by check for a purchase into a mutual fund is that we do not allow a withdrawal from the mutual fund for 10 days after the purchase. That, at least, normally prevents someone from making the purchase, bouncing their check and also making a mutual fund withdrawal in quick order.

"This is all spelled out carefully in the fund prospectus."
—Nolan North, CTP, Consultant, T. Rowe Price Associates ▲

Payments Fraud Drill Reveals Weaknesses

Jonathan Starkey

Over three days in early February, manufacturers, retailers, financial institutions and card processers participated in an exercise designed to expose weaknesses in their payments processes. The Cyber Attack against Payments Processes (CAPP), as the exercise was called, boasted nearly 800 participating organizations—and the support and participation from AFP and several members.

Bill Nelson, executive director of the Financial Services Information Sharing and Analysis Center (FS-ISAC), the group that organized CAPP, will discuss the findings of the exercise at AFP's Treasury Management Forum later this month. Nelson spoke with AFP recently about the exercise and payments fraud.

AFP: Would you explain February's exercise?

Nelson: We really wanted to test the ability of all different types of parties, financial institutions, card processors, also businesses and retailers, to respond to major cyber attacks against their payments processes. We wanted to raise awareness about the different types of attacks that are out there. In turn, after the exercise, make recommendations to improve the processes. Information sharing is our middle name. We really want to get people aware of the fact they need to share information. We had daily scenarios and questions each day and everything built on each other. For the businesses that participated, the scenarios were unique to them. But we did have a spear-phishing, Trojan account takeover scenario. We did also have a massive data breach of a fictional company that had a lot of checking account data, basically 120 million records. It was all fictional but we wanted to test that and see what the impact was. Everybody agreed that the impact was really bad. There seems to be some differences in perception between banks and businesses and maybe what some of the best remediation efforts are, or what banks think their business customers may be willing to swallow. Surprisingly, we got some pretty interesting data on what measures corporate customers are willing to take so they don't have losses.

AFP: How do you think it went?

Nelson: Many of the organizations we talked to had various teams in their organizations working on this. Some of them had as many as 20 or 30 people. In the post exercise, there was a lot of interest in doing this again and suggestions for improvements. Everybody that participates gets the full report of everything that happened, all of the four different communities that were attacked, or pretended to be attacked, with lessons learned and recommendations for risk remediation steps. We'll have summary data and we'll have an executive summary. Post-exercise, we want to continue the educational effort. There are some real gems in there, in terms of things we're starting to find.

Continued on page 6

AFP: Why now for this exercise?

Nelson: We had the account takeover attacks that the FBI brought us into back in August. There were so many businesses; this is a real problem. We've just seen more and more cyber fraud. It just seemed appropriate that we should do an exercise. We supported the Department of Homeland Security in a number of their exercises. We've supported other exercises within out sector, financial services. It just seemed like a logical thing to do our own. It was a good well rounded group of people that came up with some scenarios.

AFP: It seems that, every couple weeks, more warnings are coming about cyber fraud. How much more rampant is the threat these days?

Nelson: It's a very persistent and aggressive threat. It's not diminishing. You have to almost raise the bar in your defense strategy, as a company, as a financial institution, to protect your customers, and I think this helps emphasize the need for more radical draconian methods to stop these attacks from being successful. If they're getting more aggressive and persistent, we had to raise the bar in our defenses. The banks do, as well as the businesses.

AFP: Are you still seeing businesses or banks that are unwilling or hesitant to share information with others?

Nelson: Sometimes it's not unwillingness; it's just not part of your culture. It can't be an afterthought, as part of our incident response procedures. The people that are sharing information, our member financial institutions that are doing it a lot, we're seeing a lot more information sharing than we've ever seen. Should everybody be doing it? Yes. Are we probably seeing most of it with members that are active? Yes we probably are. I think what we're getting is pretty good but it could be better. And the government is doing more sharing. I think we're going to see more of that. ▲

News

Fed Announces Gift Card Rules

New Fed Reserve Board rules limiting fees on gift cards, and expiration dates, will take effect this August. The new rules prohibit issuers from charging dormancy, inactivity and service fees on cards unless:

1. The customer has not used the certificate or card for at least a year
2. No more than one such fee is charged per month
3. The consumer is given clear and conspicuous disclosures about the fees.

Cards cannot expire under the new rules for at least five years after the card is issued, or five years after customers last loaded money onto their card, the Fed said.

The rules cover retail gift cards to be used at a particular store (or stores) and gift cards branded by a particular network, such as Visa, which can be used anywhere that brand of card is accepted. ▲

Continued on page 7

Wells Fargo and Visa Team on Text Alerts

Wells Fargo and Visa are collaborating to provide customers with text alerts of potential fraud. Visa's VisaNet processing network will send out the alerts on behalf of Wells Fargo when a transaction meets certain criteria selected by the bank's card customers. The alerts will be sent within seconds of transactions.

According to Wells Fargo and Visa, the criteria a customer may select include:

- Transactions that exceed a dollar amount chosen by the cardholder
- Transactions initiated internationally
- Card-not-present transactions, such as purchases made online or by telephone
- Cash withdrawals from an ATM machine
- Declined transactions
- Gasoline transactions.

"We believe Rapid Alerts will give customers added peace of mind that they will be notified almost immediately when transactions occur," said Peter Ho, product manager for Wells Fargo Card Services and Consumer Lending. "We piloted Rapid Alerts in 2009 and received an overwhelming positive response from participants who said text alerts were an invaluable tool for monitoring their accounts. We want to help our customers succeed financially, and this is just one more tool to help them get there."

Alerts will include the time and date of the transaction, as well as the amount, currency conversion and merchant information. The alerts won't just help identify fraudulent transactions. They should also help customers mandate and track spending, Wells Fargo and Visa say.

"Visa is empowering cardholders to take an active role in managing and protecting their Visa accounts," said Jim McCarthy, global head of products at Visa Inc. "Visa's ability to analyze transactions 'in-flight' enables us to provide our cardholders with near real-time transaction alerts. Participating Visa cardholders can typically receive alerts before they walk out of the store, rather than hours or even days later."

Visit rapidalerts.wellsfargo.com to learn more. ▲

CHIPS Turns 40

CHIPS, the wire transfer network operated by The Clearing House, turned 40 on April 6. The network started with nine participants trading payments no larger than $10,000. Today, CHIPs processes 350,000 payments daily, valuing $1.5 trillion, for 48 financial institutions in 22 countries, including 95 percent of all international U.S. dollar clearing.

"Since it went live on April 6, 1970, CHIPS has dramatically changed the landscape of payments systems and has become a critical part of the global economic infrastructure," said Rossana Salaris, senior vice president for payments products at The Clearing House.

Discussions about creating CHIPS date to 1966, when a successful payment automation study ultimately led to the creation of the Clearing House Interbank Payment System (CHIPS). ▲

B2B AP Best Practices

Matthew Dragiff

Although cyber fraud is on the rise (see page 1), the *2009 AFP Payments Fraud and Control Survey* revealed that over 90 percent of responding organizations were victims of old-fashioned check fraud. Almost 50 percent of those organizations suffered a financial loss from check fraud.

Despite the sobering numbers, many organizations still issue checks for B2B payments. This time-consuming, inefficient practice becomes more expensive as the costs of postage, paper and supplies continue to rise. When combined with the financial loss from check fraud, there is a compelling business case to accelerate the migration to electronic payments.

With the massive effort that goes into issuing checks, many companies need to be reminded that the function is not core to their business. It is something that can be outsourced. Best practice outsourced payment solutions offer features that can reduce risk from check fraud while providing a comprehensive integrated solution for check printing and delivery, and could help remove the traditional barriers that have blocked electronic payment adoption.

Best practices

Here are some industry best practices for efficient AP processing and fraud reduction:

Centralized AP processing ensures that all of an enterprise's outgoing payments are transmitted through the same system. This provides increased transparency, a common workflow-controlled release process, simplified auditing and compliance, and a reduction in bank connectivity requirements. A best practice outsourced solution can function as a Corporate Payment Transaction Platform that allows organizations to centralize payment execution and integrate payment processing for all payment methods–check, ACH, wire and card.

With centralized payment execution comes the ability to consistently implement fraud prevention best practices including multiple levels of approval, segregation of duties, check stock inventory management and payment analysis. Configurable security controls can be used to restrict access levels of specific users within the payments application. One user may be allowed to submit a payment file for processing while another is required to review and approve payments before releasing them for processing. This is especially helpful for organizations without an ERP system that provides AP approval workflow. While some companies may utilize their bank's proprietary Web portal for multi-level approval, this becomes cumbersome with multiple banking relationships because employees will be required to login to multiple systems. With one system employees have one centralized Web portal for payment review and release.

Reducing check fraud

Minimizing check handling reduces the opportunities for fraud. Outsourcing check printing helps by eliminating employee access to check stock and check handling between printing and mailing. This dramatically reduces the opportunities for employees to steal and alter an outgoing check to a vendor, to steal blank company checks, or to steal and misuse obsolete check stock.

Centralizing bank connectivity through an outsourced solution eliminates the need for the IT organization to develop the data feeds necessary to take advantage of bank services such as positive pay or payee positive pay. These services are well accepted, strengthened fraud control measures that achieve greater security by providing additional points of comparison between checks presented and checks issued.

Today more than ever, companies are looking for ways to decrease expenses, become more efficient and reduce fraud. For this reason, many corporations are now looking closely at their payments strategies. Best practice outsourced payment solutions assist organizations in their fraud prevention strategies by implementing less manual processes that are also more transparent.

Another important benefit that an outsourced solution can bring is the ability to transition corporate accounts payable disbursements away from the inefficiencies surrounding paper checks and manual processing. In addition to decreasing costs, improving transparency and minimizing fraud, organizations that outsource their payment processing free themselves of this cumbersome task, allowing them to better focus on their core competencies. ▲

Matthew Dragiff is the Director of Product Management for AvantGard Payment Services