

Payments Fraud

By Stephen Markwell

August 2010

The following podcast is brought to you by J.P. Morgan.

Debbie: Hello, and welcome to a podcast on payment fraud. I'm Debbie Hartley, and I'll be your moderator for today. I have Stephen Markwell, Senior Product Manager of Treasury Services Payables today. Welcome, Stephen.

Stephen: Thanks for having me, Debbie.

Debbie: Let's get right into it. Who is at risk of payment fraud, and what is at stake?

Stephen: Payment fraud is a big issue, and it's impacting most of us in one way or another. In fact if we look over the last five years consistently, year over year nearly three quarters of businesses are victims to either payment fraud losses or attempts. And we can break that three quarters down a little more discretely and say that organizations that earn over 1 billion in top line revenue, 80 percent of those are victim to payment fraud losses or attempts. And those with under 1 billion in top line revenue, 63 percent of those were victim to payment fraud losses or attempts.

And it's also a growing issue in terms of attempts. I talked about the fact that about three quarters of organizations were susceptible to fraud losses or attempts pretty consistently over the last five years. One of the issues we're seeing is that those 73 percent are being impacted with attempts more frequently. So last year nearly 30 percent of organizations reported an increase in attempts.

We can also look at what's at stake in dollar terms. Last year, the median client loss per occurrence was \$17,100, and that's up from 2008's figure, which was \$15,200. I think one of our challenges is to convey the value of fraud protection to upper management. You know, fraud exposure, fraud protection — these are ambiguous terms. It's sometimes difficult to build them into a business case, but we can use this number and say, okay for an average account buying a basic set of fraud protection services, you can now protect yourselves with moderate fees for over 20 years before you become even close to that \$17,000 figure. I think that's a good insurance policy.

And then lastly in terms of aggregate losses, we have a report from the FBI that shows consumers and businesses lost over 20 billion dollars in payment fraud a year. And that's a big number. And it's also excluding mortgage fraud, which is a growing figure.

Debbie: And that is a growing risk. Are certain payment types more vulnerable than others?

Stephen: They certainly are. Check volume as a percentage of total payments has decreased by 18 percent —from 2003 to 2006, and it's expected to continue decreasing by 7 plus percent a year. That leads us in the direction of thinking that maybe it's not the most pervasive type of payment vehicle. Having said that, the value of checks is increasing, so check does remain the number one vehicle for payment fraud. As it turns out nine of ten organizations that experienced a fraud attempt were victims to check fraud. We also know that 89 percent of those that were victim to check payment fraud, reported an increase in attacks. So before I talked about in aggregate about 30 percent said there was an increase. For those that incurred a check fraud attempt, 89 percent of them saw an increase in attempts. That's a big number. And then 64 percent of payment fraud victims report that checks resulted in the largest dollar amount of loss.

Debbie: Why are checks more vulnerable to fraud, and what can organizations do to protect themselves?

Stephen: First, a check is typically a paper negotiable item that we stick in an envelope and, send to our payee via postal mail. So here you have a paper item that has your account number and your routing number on it. It's circulated via postal mail, so it's certainly easier for fraudsters to steal versus stealing electronic information. — To create a counterfeit check does not really require specialized skills or deep subject matter expertise. There's a lot of technology out there today that helps fraudsters commit this crime. Tools like desktop publishing and laser printers. And so just in terms of, you know, financial solution best practices, if you're writing checks against your account, Positive Pay with Payee Name Protection is certainly the strongest form of fraud protection. If you're not writing checks against your account, and that includes depository accounts, Post No Checks is also one of the strongest forms of check fraud protection. Having talked about, , some of the strongest forms, we always have to right size these fraud protection solutions to our own organizations and our own internal constraints.

Another solution is Reverse Positive Pay. If you have constraints around the amount of fees you can pay for protection, or the resources you have available to submit timely issuance, Reverse Positive Pay is a solution to consider. In general it costs about two thirds to one half of what Positive Pay does. You don't have to submit issuance, but we basically send you a list of all of your items that were presented for payment in the last 24 hours, and you can make a pay or return decision. So that's the great side of the story. It does require you to be diligent and look at all of those exceptions and make decisions, and it's also not a great solution if you have to allow your non-bank account holders to cash checks with your financial services provider.

Debbie: And what about fraud trends and solutions across electronic forms of payment, like ACH and card?

Stephen: Certainly susceptible as well. ACH fraud is growing; three of ten respondents this year reported an attempt or loss. The good news for ACH is that only 11 percent of those suffered a financial loss, but times are changing. ACH continues to grow in popularity. There are two solutions we recommend and one is ACH debit block. It's growing in popularity. In 2008, 71 percent of respondents were using it. This last year, 77 percent are using it. . And you have a couple of options. You have the hands free option as I call it, which is to block all. You may have a depository account and you never want to accept an ACH debit, so you may block all ACH debits. You set that rule up once. Anytime a debit comes against your account it never posts. You don't have to pay or return anything. It just goes away. That is a great tool if you know you're not going to accept debits. You can also create an include list. So if you have a payroll account, and you know that only a payroll vendor is going to debit your account, you can say, "Hey, this payroll vendor is the only one that I'll accept payments from." And all other ACH debits would be systemically rejected.

That's a great tool if you have little or no variability in who you're making payments to. There's also an option called the exclude list. You're basically saying who you won't accept debits from. This is something that we warn clients against. While it does a great job of stopping debits from those clients, or those vendors, it does not stop the new fraudster who you have yet to meet.

The other solution that we talk a lot about is ACH debit filtering. You're also hear it called by different names, by different institutions. Sometimes it's referred to as ACH Positive Pay, or ACH Transaction Review, but this is growing as well. In 2008, 55 percent of respondents were using the service, and in 2009, 58 percent were using it. This tool just gives you a little more flexibility. With this service, you set your criteria. Examples of criteria include a company ID list, debit or credit, dollar value threshold, a standard entry class, which is the type of ACH transaction. You define this criteria and anything that doesn't match your criteria appears to you as an exception, and then you can make a pay or return against those items. So ACH Transaction Review is different from ACH Debit block in that transactions aren't automatically rejected. They basically are compared to your criteria. If they don't match, you get a chance to look at them and make that pay or return decision. This is a better solution if you have a lot of variability in your vendor payments as it ultimately helps you to retain that visibility and ultimate control over who you pay and who you do not.

You also asked about credit card fraud. It's up as well. It's up from 18 percent in 2008 to 20 percent in 2009. Let's talk about B2B card attempts. Purchasing cards at 72 percent and T&E cards at 45 percent were the most prevalent. Out of all of these credit card fraud losses, fully 27 percent of that was committed by an employee or someone internally.

A lot of that is attributable to T&E card abuse. There are many types of T&E card abuse. Just a couple of examples — an employee can make an unauthorized charge and then they can mask it or categorize it as something that it really was not, and it may slide thorough your system that checks for those types of red flags. Another one is to blatantly make an unauthorized payment with your T&E card and then to deny that you ever made that payment. You could report that the card could have been lost as an example.

In terms of best practices with credit card, certainly segregation of duties, which we'll talk about later as an internal practice across all payment vehicles. You can segregate duties by purchase request, authorization, execution, approvals. Consistency is a big deal with mitigating credit card fraud. If you promote consistency across your

organization, across the different lines of business, and do that in terms of consistent card issuance policies and procedures, consistent transaction controls, usage controls, it really becomes much easier on you to find those exceptions.

Education is very important, if you have a strong program around educating your employees and your managers around policies and procedures, it will go a long way towards reducing those exceptions or those red flags that we talk about.

And then there are many protective controls and we've talked about some of them. Transaction limits — you can have a transaction limit by category. You can have monthly limits, and you can block unauthorized vendors. You can even go as far as to define custom red flags. An example here would be that you could add increased scrutiny around use of T&E purchases for entertainment vendors. As an example, you could have those transactions routed to the employee's manager and require a second layer of approval.

Debbie: Thanks, Stephen. You mentioned internal controls. So what are some of the best practices that organizations can implement to help mitigate payment fraud risk internally?

Stephen: I think it helps to think about fraud exposure in terms of this open window. Fraud solutions that your financial services provider offer, they certainly help to close this window to a great degree, but you still need a strong suite of internal controls to pull that window down until there is only a very thin crack.

When you think about all of the handoffs in the life cycle of a payment, these fraud solutions help, but ultimately we're only as strong as our weakest link in the process. One best practice, and this was highlighted by 90 percent of respondents, was the segregation of duties. If the same person is signing checks, uploading issue information to the bank, approving exceptions, then you essentially have no strong form of fraud protection. When we think about the full life cycle of the payment, the payment may be authorized, it may be originated, advice is sent to your financial institution, your financial institution compares your advice to what was presented and they create exceptions. Those exceptions are sent to you and decisions are made to pay or return. All of those are gateways or checkpoints. And the best practice here is to segregate duties at each of these gateways and add a second layer of approvals.

Like we talked about earlier, you have to right size this recommendation to your organization. If you're a small business — a family owned business, you may have one controller. So it's not feasible to have 15 people administering this process. The most important point of segregation of duties is to really make sure that the same person that is issuing payment is not approving exceptions as well.

Another best practice that is very effective, is segregation of accounts. You can segregate your account by purpose. An example of this is you could have a payables account, or an account that's earmarked just for receivables. You can segregate your accounts by payment vehicle, so accounts that are used solely for check, solely for ACH, solely for wire. You can also do it by value and volume, you know, high versus low. The idea here is that if you isolate activity on your accounts by all of these factors, you can then protect your accounts from all payments that don't meet this criteria. And then conversely, if you don't do this, if you have one large operating account that's used for many purposes, many payment vehicles, high value, low value, if the volume fluctuates wildly — defining an exception becomes very difficult.

Another best practice is centralized fraud protection governance. I've seen many large organizations use this model. These governance organizations are a central point of contact when a fraud loss does occur. They perform an exhaustive root cause analysis on the loss to figure out what in the process broke down. They're a central point of communication, so they may push out communication around new fraud scams to employees. They can also aggregate best practices so as a line of business identifies a best practice, it's submitted to this governance board that reviews it, vets it across the institution, and eventually institutionalizes that best practice as something that the entire organization uses.

There are many best practices around HR, and I'm not a subject matter expert here, but a few of the practices that many large organizations have advised me of is forced vacations. If you have an operate staff, a best practice is to force vacations for a period of time from one to two weeks. Another one is to actively rotate jobs, so to move operators into different positions. The idea here is basically that if you have individuals that have the same job for 30 years, and they haven't taken vacation in the last 10 years, you're creating an environment that makes it very easy for them to commit fraud, to integrate funds, to layer funds, to such a degree that by the time you figure out that money is missing, it's too late.

And then lastly, when we think about this in broad terms, we've talked about some of these payment types like ACH and wire gaining wild popularity. When you think about how quickly technology is advancing today, and as we look at the rate of fraud scheme innovation, and the fact that it's increasing dramatically, it starts to become pretty easy to see

that fraud protection is not a static target, but rather it's one that requires constant monitoring for new trends and innovation. It requires rigorous internal controls, and these are controls that you frequently reevaluate, that you frequently update. And ultimately it requires a financial partner that's both serious about investing in fraud protection innovation, and serious about educating their clients.

Debbie: Thank you, Stephen. That's very helpful information to stay ahead of payments fraud. The statistics that Steven mentioned come from the 2010 AFP Payments Fraud and Control Survey that was sponsored by J.P. Morgan. To download the survey and for additional information on payments fraud, please visit J.P. Morgan's payment fraud resource center at www.jpmorgan.com/preventfraud.

J.P. Morgan is pleased to have brought you the proceeding podcast. For more information on J.P. Morgan Treasury services and products visit our website at www.jpmorgan.com/ts.