CAUTIONARY TALES: WHAT AP CAN LEARN FROM 3 REAL-LIFE PAYMENT FRAUD EXAMPLES

IOFM Institute of Finance & Management

Sponsored by

Paymode-X

CAUTIONARY TALES: WHAT AP CAN LEARN FROM 3 REAL-LIFE PAYMENT FRAUD EXAMPLES

It's not hard to find stories about the devastating impact of accounts payable fraud. Government and business sites cover them constantly, and big consumer news channels even feature the more spectacular ones.

If it seems as though fraud cases are increasing, it's because they are. Strategic Treasurer notes in its 2022 fraud report that AP departments are the most vulnerable to email scams, with 73% listing it as their number one fraud concern. And one independent security analysis firm notes that business email fraud attacks ramped up by nearly 23 percent in the last year.

Fraudsters trick AP staff into handing over login credentials or changing vendor information to pay their scam accounts.

That rise is possible because fraudsters are becoming ever more resourceful. They get better and better at stealing information, often convincing unsuspecting finance staff to just hand critical data over without even being aware that they did so. And these criminals are grouping up, forming organizations that work as a unit to expand their criminal activity on a widespread – even global – level.

Even a couple of savvy people or even a single individual can do a lot of damage to your business before their scam is uncovered. Unfortunately, by the time you catch on, you may be out of a lot of cash. In many cases, even when the fraud is detected and the perpetrator caught, the money is never recovered.

What to do? Chris Gerda, Risk and Fraud Prevention Officer of Paymode-X, notes, "While training AP staff to be mindful of the different ways in which fraudsters operate can be helpful, it certainly doesn't make you bulletproof. Sometimes, the scams are so well-crafted that they're almost impossible for a human being to detect."

Let's discuss three types of B2B payment fraud and provide real-life examples of how AP staff have fallen victim to these schemes.

Business Email Compromise

A term you'll often hear is "social engineering." But what is it and how do scammers use it to defraud you?

According to Gerda, "Social engineering is convincing people to do something they otherwise should not do." Simply put, fraudsters find ways to trick you into trusting them, often by pretending to be someone you know. They may purport to be the human resources department asking you to log into their new employee portal and then stealing your credentials, or masquerade as the CEO asking you to submit an urgent wire transfer overseas.

Social engineering is a method of manipulating people to do something they shouldn't.

The most sophisticated of B2B business email compromise (BEC) scammers target businesses because of the potential reward, hoping to uncover a weakness that allows them to steal large payments without being detected. In fact, the FBI recorded $43 billion of BEC-related losses on a global scale over five years. It's big business — and fraudsters get better at scamming AP staff all the time.

Here's one recent notable example. A man in Charlotte, North Carolina was convicted of defrauding six companies in a money mule scheme using BEC. Using fake documents and various aliases, he opened numerous bank accounts to be used as pass-throughs for laundering stolen money. He set these up with small initial deposits and then utilized them to receive big-dollar wire transfers from the U.S. companies he tricked into paying him because he was impersonating their real vendors. Within a short time of receiving the fraudulent payments, he would again use fake identities to make large cash withdrawals, purchase official checks and wire money to other bank accounts he controlled to make the trail of stolen funds hard to trace.

Overall, he stole $2 million from the targeted businesses. While he was eventually caught and convicted on multiple counts of money laundering and identity theft, it's uncommon in such cases for the businesses to recover all their stolen money, particularly when wire transfers are involved.

Account Takeover

Once an AP team member's credentials or emails have been compromised, a fraudster may then access internal communications, the payment system, vendor management systems, bank accounts — even cryptocurrency wallets, if your company uses crypto.

Once a scammer obtains an AP employee's login credentials, they can do everything the employee can.

This puts incredible power into the scammers' hands, as they're able to do everything the employee whose account information was stolen can do. Whether they access your company's payment data, or even get hold of customers' banking details that are contained within your vendor master file, they can do tremendous damage. And that damage isn't only to your bottom line, because if they steal from your suppliers due to lax security on your side, your business relationships may well be ruined.

Here's a case that shows just how clever fraudsters can be when it comes to account takeover — an example of a multi-phased scheme that required a good bit of creativity. Here, the perpetrator managed to convince mobile phone carriers to provide him with SIM cards with his victims' cellular phone numbers on them; these were then inserted into phones in his possession. This enabled him and his cohorts to gain access to the victims' email and crypto accounts, which they helped themselves to.

This has huge potential consequences. Consider how you use your phone for business. If you regularly communicate with your AP team via phone-enabled email, use it to approve payments, or even utilize a two-factor authenticator app on it, all that could be compromised. With our heavy reliance on our mobile devices to do business these days, having your SIM hacked could represent a major threat to your organization — and in this case, that happened without the targets ever losing access to their physical devices.

To top it all off, in this example, after the thieves stole from their victims, they then blackmailed them to get their confidential information back.

Imposter Vendors

This is exactly what it sounds like: fraudsters pretending to be somebody they're not.

This is easier in some industries than others. For instance, names of stakeholders involved in large contracts such as construction projects are usually public information, and these invoices tend to be big-ticket ones.

Here's how this type of fraud works. A scammer will pretend to be a legitimate vendor whose name you recognize. Because they may have been monitoring your correspondence behind the scenes through BEC, they learn to carry on a cordial conversation through email that seems to be coming from a known entity you've communicated with before. Once they've got you convinced they are who they say they are, they may request a payment that directs the funds to a scam bank account or ask for a wire transfer, which is generally irrecoverable once it's sent.

Gerda explains a real-life example of an imposter vendor's attempt to steal from a construction company. "They experienced an email breach they were unaware of. The fraudster sat back and watched emails for a while to familiarize himself with the situation, then tried to get the payer to send a large sum to a scam account."

One company was completely unaware that their email was being breached on an ongoing basis.

Because the fraudster had access to the company's accounting email, he carefully set up forwarding rules to redirect specific correspondence to himself and deleted his sent emails so that the accounting team was unaware that this was going on right under their noses. There was no obvious evidence within the compromised email account that this correspondence had ever occurred. The scammer even changed the phone number in the email signature in case AP felt the need to call.

The victim organization in this case was fortunate. Its AP department uses Paymode-X to securely pay suppliers. Using a multi-faceted, layered security approach, the solution digitally authenticates new vendors and verifies existing vendors using sophisticated technology. The built-in security measures detected the threat and prevented

the fraudulent payment, one that an AP staff member fully believed was for the real vendor.

As one Paymode-X customer observes, "We chose this solution because it verifies and validates the banking information of our vendors. We are no longer responsible for maintaining vendor banking details."

5 Ways to Prevent B2B Payment Fraud

By now, it should be obvious that even the most diligent of AP staff can't always prevent fraudsters from working their scams. They have neither the time nor the training to manually investigate and thwart these attempts, many of them quite clever. Here are five key things you should know about fraud prevention.

1. **Monitor email traffic through technology solutions and staff training.** As we've seen, in the case of many reported scams, the problem begins with email — stolen credentials or spoofed messages that lure you into making payments to a fraudulent vendor. Understanding when an email comes from outside your organization, contains malicious links or is spoofed takes solid training and a good email monitoring tool.
2. **Verify supplier phone numbers.** One of the tricks scammers use in compromised emails involves the fraudsters substituting their own phone numbers in the signature, just in case you decide to call in order to verify their identities. The phone numbers should be checked against up-to-date vendor contact information stored outside of email (in your vendor master file, for example, or through online research) to ensure they are coming from the business they purport to be.
3. **Use a highly secure online portal that your solution provider has set up to evaluate each vendor's legitimacy behind the scenes.** This should be an extremely thorough process that will prevent you from making bogus payments by eliminating emailed payment requests and changes to contact information. For example, a top-notch solution will automatically check domain name registration information to determine who the domain is registered to, and how long ago was it registered.
4. **Confirm supplier banking information.** Your solution should also verify vendor banking information so that you can rest assured your payments aren't being sent to a sham bank account opened by a fraudster. As mentioned in the money mule example above, once payments are deposited in a fraudster's bank account, the perpetrator will often move them around to make it next to impossible to trace or recover them.
5. **Establish an internal incident reporting process.** If you're involved in processing payments, it's critical that when you see something suspicious, you have the ability to stop or slow down a payment or a change to vendor information until it is deemed safe. "There are many payment methods out there," says Gerda, "but the most efficient one is, first and foremost, the one that's most secure, regardless of type — be it card, ACH, RTP — and all the ones we still have yet to see."

Technology Is Your Ally

"While it's always important for your team to remain on guard when it comes to fraud, technology is your best weapon when it comes protecting your business — and your cash," says Royce G. Morse, IOFM Managing Editor. "Expecting staff to have the resources and time to dig down into each invoice to verify that it's safe to pay is not reasonable, either in terms of the time or the expertise required to do so."

A layered, automated approach that considers many different factors is the most secure protection against fraud.

Instead, the security provided by a highly advanced payment system like Paymode-X establishes a technology barrier between your payments and fraudsters, one that's extremely difficult to breach. That removes the social engineering pathway that many fraudsters use to trick staff into giving out information or making high value payments to them, thereby shutting down the most lucrative avenue for external fraudsters.

Taking a layered approach against fraud risk is the most secure method of protecting your company's cash. Many aspects of each transaction can be analyzed and flagged

behind the scenes, from IP addresses, bank authentication and device fingerprints, to digital identity and more. This thorough technological approach makes it nearly impossible to perpetrate a scam, which in turn keeps your vendors safe, your data private and your team focused on their tasks.

"In the past four years, Paymode-X has been successful in securing well over $1 trillion of B2B payments against fraud attempts using digital authentication strategies" says Gerda. "In that time, we've blocked hundreds of direct BEC fraud and fraudulent vendor attempts." In fact, Paymode-X maintains an authenticated network of over 500,000 vendors who are used by some of the largest corporate, bank and government entities in the U.S.

That proven track record cannot be beat. Don't rely on your team to try and thwart devious scammers. Instead, fight back with sophisticated technology which is your best line of defense.

About Paymode-X

Bottomline is at the forefront of making complex business payments simple, smart and secure. We help over 600,000 companies in 92 countries around the world by automating and securing core accounts payable and accounts receivable processes through solutions including Bottomline's Paymode-X.

Using Paymode-X, organizations overcome rising costs, inefficiencies and sunk time caused by manual AP processes by automating supplier invoice and payment methods. Paymode-X is the largest B2B electronic payment network, processing over $300 billion per year to more than 500,000+ businesses, all with zero fraud and offering cash-back rebates on ACH and card payments.

Learn more at www.bottomline.com.

Paymode-X | Powered by Bottomline

About the Institute of Finance & Management

Accounting and finance professions have each undergone nothing short of a complete transformation since the Institute of Finance and Management (IOFM) was founded in 1982 and since then our mission has been, and continues to be, to align the resources, events, certifications, and networking opportunities we offer with what companies need from the accounting and finance functions to deliver market leadership. IOFM empowers accounting and finance professionals to maximize the strategic value they offer their employers.

Our enduring commitment to serving the accounting and finance professions is unmatched. IOFM has certified over 25,000 accounting and finance professionals and serves several thousand conference and webinar attendees each year.

IOFM is proud to be recognized as the leading organization in providing training, education and certification programs specifically for professionals in accounts payable, procure-to-pay, accounts receivable and order-to-cash, as well as key tax and compliance resources for global and shared services professionals, controllers, and their finance and administration (F&A) teams.

Learn more at www.IOFM.com