3 WAYS FRAUDSTERS COMPROMISE AP SECURITY AND CONTROLS—

And how you can mitigate the risk

IOFM Institute of Finance & Management

Sponsored by

Bottomline

Have you ever received an email from a vendor that was hacked? This is a common situation, particularly for accounts payable organizations that make large-dollar payments.

The fraudster may have compromised the vendor's email to secretly view correspondence about a particular transaction, then intervened prior to your payment run by emailing you from the vendor's account and requesting a change to the banking information. They covered their tracks by deleting sent emails, setting up automatic forwarding rules and changing the phone number in the vendor's email signature to intercept the call you're likely to make to confirm the banking change.

Now throw in the post-pandemic confusion about accepted procedures and security measures within AP, and the scammer has an even greater likelihood of successfully intercepting that large payment. How can you protect your organization from this and other frightening fraud scenarios?

Finding a Payment Fraud Vulnerability

Fraudsters thrive on disruption, which opens the door to process and technology vulnerabilities. That situation is now playing out across the country as businesses are looking to reopen their offices and move staff back in-house post-COVID.

Fraudsters thrive on disruption, which opens the door to vulnerabilities.

Many organizations are also looking at a hybrid workforce, with some employees working from the office and some working from home, or allowing flex schedules that only require staff to go into the office a few days a week. What that means is that fundamental AP processes like invoice receipt, processing and approvals will be in flux as all that gets sorted out. It also raises the question of whether the staff is working with standard-issue equipment or on personally-owned devices—and whether the right security measures are protecting all that different technology.

Ever on the lookout for opportunities, you can bet that thieves and scammers will find new ways to exploit the situation.

"The shift to in-office or hybrid policies is going to drive fraudsters to come up with new, imaginative schemes to try to defraud companies," says Chris Gerda, Bottomline Technologies' Risk and Fraud Prevention Officer. "We're not used to working in the office after a year or more away, and if you think that's not going to impact your security, think again."

A Case in Point

Policies and procedures are important, of course, but it's likely they all need to be rewritten at this point, if they haven't been already. Of course, just having these measures in place isn't enough to protect your organization—they must be followed rigorously. That requires training and oversight, something organizations have had little time or opportunity to do in the current chaotic business environment. It also requires flawless execution, not to mention considerable effort.

Policies and procedures alone won't protect your business against fraud.

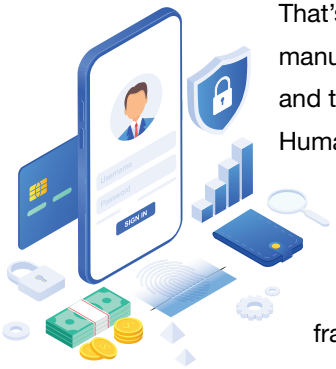
All that is iffy, at best.For example, the town of Peterborough, NH recently lost $2.3 million after cybercriminals tricked a town employee into sending large payments to the wrong accounts.

How did it happen? An overseas fraudster impersonated an established high-value vendor and emailed the AP department with a change to banking information. This classic scam enables the thief to redirect payments to a personal account, withdraw the money, close the account and disappear.

In this case, multiple emails were used to impersonate different individuals to gain credibility. The accounts payable coordinator changed the banking data without calling the vendor to confirm it.

Peterborough town officials learned of the sophisticated fraud scheme when a vendor they sent payment to alerted them they did not receive their monthly transfer from the town. Officials said at that time they realized the town was the victim of business email compromise fraud.

Peterborough's finance department quickly tried to stop payment, but the funds had already left the town's bank account. At the same time, their IT staff followed protocol for alerting the U.S. Secret Service and kicking-off investigations into the email-based payment fraud scheme.



That's the problem with relying on manual systems, policy compliance and the vigilance of employees. Human error, confusion and pure laxity can leave a business wide open to getting scammed.

For this reason, effective fraud prevention in the current payment environment shouldn't be left to manual processes and staff to enforce. It needs to be implemented through automation and digital authentication strategies instead.

The Three Types of Payment Fraud

Fraudsters generally employ one or more of these high-level tactics to scam AP organizations into making fraudulent payments:

1. Business email compromise (BEC)

The scammers either gain access to your vendor's email, send "spoof" emails, or even create web domains appearing to mimic the real business. What does this look like? Simply put, it's when AP receives an email that appears to be from a vendor, instructing staff to make a last minute bank change before a payment is sent.

These hacked emails come from the phishing attempts we consistently see, sent with the intention of obtaining user name and password information. Fraudsters will send a seemingly innocent email that states, "Corporate HR is asking all employees to re-validate their contact information as we move back to the office. Login with your credentials to confirm." Gerda says, "Beware of anything that asks for credentials."

2. Account takeovers

If a scammer does obtain your login credentials through phishing or another method, this information can be used to log into your AP system, bank accounts, vendor management systems and emails in order to initiate and approve bogus payments, change banking information to misdirect payments, or even steal vendor banking information and other sensitive data. Keeping your vendors' bank information in a secure, encrypted way is critical.

Keeping vendors' banking information secure and encrypted is critical.

3. Imposter vendors

Here, new vendors you're in the process of onboarding are impersonated by a fraudster seeking to intercept the first payments—they use emails, phone numbers and names that are similar to vendors' real information in order to impersonate them. If you have vendors who bid on public contracts, they are at particular risk, since fraudsters know exactly who to impersonate to obtain a payment in the new relationship.

Fraudsters are highly creative and determined to exploit your vulnerabilities.

Protecting Yourself

As we've seen, fraudsters are highly creative—and determined—when it comes to detecting and exploiting your vulnerabilities. They're enabled by the inadequate information analysis performed in the traditional vendor onboarding process. Here's where a strong defender like Bottomline's Paymode-X (PMX) can bring the digital verification expertise required to stop sophisticated fraud attempts in a modern and everchanging payables world.

Paymode-X uses an online enrollment portal that includes multiple layers of security and bank-standard encryption methods for all banking information. Before adding records to the vendor master file, the solution thoroughly vets each supplier, and afterward, any changes to banking information are validated each time. A simple example of this is the way PMX reviews IP addresses for aberrations and geolocation proximity, and bounces them against a robust blacklist of known bad IP locations.

Leading payment solutions use "device fingerprinting" to verify legitimate transactions.

Paymode-X employs a defense-in-depth strategy, where no basket ever contains all the eggs, by using different types of multi-factor authentication, combined with sophisticated behavioral analytics to help keep your information safe. It does this by using a blend of critical digital information, enhanced with additional data sources designed to detect red flags that reveal that the business is not who they say they are. For example, communication coming from a pre-paid "burner" phone being used as a contact number for a new vendor that purports to be a large corporation is an obvious indicator of payment fraud.

Leading payment solutions also utilize "device fingerprinting." An application like Paymode-X learns about known devices, from phones to computers—so it can recognize them before allowing a bank account update or change to contact information from those sources. Changes coming from known devices are less risky than those coming from unknown sources, which require additional validation.

Paymode-X also performs ongoing OFAC checks, which is a cornerstone of any company's good payables program; this ensures you aren't doing business with prohibited entities and countries. Doing so can result in significant fines and penalties—which in recent years have been levied against corporations who have their own independent responsibilities to verify their vendors.

The Power of Secure Cloud Technology

A major advantage of using a cloud-based solution like Paymode-X is that it's available on any internet-connected device. That means that work-from-home staff, office users and people on the road can all use the application from their devices—desktops, laptops, tablets and phones. If approvers are traveling, they are still able to approve invoices from their mobile devices, keeping the payments flowing and the vendors happy.

All payment activity should be protected by comprehensive cybersecurity.

That also means that no matter where AP staff or approvers are working and on what device, their activity is protected by comprehensive cybersecurity. This is particularly important now when staff is in a state of transition, because whether they remain remote, go back to the office full-time, or transition to a hybrid home/office working arrangement, that security is needed.

How's that working? Let the numbers tell the story. Paymode-X holds an authenticated network of over 450,000 vendors being paid by some of the largest corporate and government entities in the U.S. Combined, they make over $250 billion in payments annually, and over the past three rolling years, PMX has been successful in maintaining a network free of fraudulent payments, while blocking a significant number of attempts—attempts that would have led to fraudulent payments ranging in the thousands to many millions of dollars. As further validation, Paymode-X is the preferred B2B payments network of seven of the largest banks in the U.S.

Fraudsters are increasingly sophisticated and harder to spot.

Fraudsters look for weak links and soft targets—and are increasingly skilled "social engineers," preying on unsuspecting staff who may be too busy to notice something that looks reasonably convincing on the surface. Fraudsters are also making technology advances that make them harder to spot, even with sound policies in place; therefore flexible, proactive digital authentication must be part of a modern payments strategy. Managing payables with an automated AP solution like Paymode-X strips away the tactics that enables thieves to be successful.

Payment efficiency depends on designed-in fraud prevention.

Gerda says, "The most efficient way to send a payment is securely through networks where fraud prevention is first and foremost in all design. As payments modernize and become faster, authenticated supplier networks and digital security tools are the key pillars to make speed safe in a changing fraud landscape."

About Bottomline

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.

At our core we share ideas, innovate and support each other personally and professionally. Doing the right thing, working with and for one another, and innovating constantly are our guiding principles, which help us achieve our common goals of exceeding expectations and delighting customers.

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

IOFM Institute of Finance & Management