Tips, tools and tactics for detecting and preventing business fraud

Aided by digital tools, too-lax safeguards and old-fashioned psychological manipulation, thieves are perpetrating sophisticated financial crimes that cost businesses millions each year. Here's what to watch out for — and what you need to do to ensure your organization's financial security.

Many organizations are well aware of common fraud schemes and how they work, but business-related fraud still happens at an alarming rate. In fact, every year, businesses around the world lose roughly 5% of their revenue to fraud, according to the Association of Certified Fraud Examiners (ACFE), and it's often those organizations that are least able to weather a financial hit of this kind that fall victim.

In fact, the ACFE reports that small businesses are among the most frequent victims of business fraud (accounting for 28% of all financial fraud), and that companies with the fewest employees tend to suffer the highest losses.

The prevalence of fraud and the sheer volume of the dollars it claims each year are sobering. But what may be even more concerning is how long it takes for cases of fraud to be discovered. The same ACFE report revealed that typically fraud goes on for a full year before it's ever detected, causing average losses of around $8,300 per month. When it comes to a data breach, IBM reports that, on average, it takes 207 days for organizations to identify a breach and 70 days to contain one.

Taken together, these facts make a compelling argument for a multi-pronged suite of solutions: Instituting a well-crafted digital safeguard to beat back attempts at internal and external fraud, and designing a thoughtful and thorough employee education program detailing the threats that exist both within and beyond the confines of your company.

Luckily, Wintrust can help with both, starting with this guide to three of the most common and pernicious fraud schemes at work today, with commentary from two of Wintrust's foremost experts on fraud detection and financial security: Ezra Jaffe, Executive Vice President of Treasury Management, and Ray Olsen, Senior Vice President of Fraud Management. **Here's what you need to know.**

WHY FRAUD HAPPENS

The most common reason why fraud flies under the radar? In 29% of cases, it's a lack of internal controls. In another 20%, it's employees overriding the internal controls that are in place.

SCHEME NO. 1

Phishing and business email compromise

Every day, a slew of emails come through the average person's inbox, and it's this overwhelming volume — combined with our desire to wade through it quickly and our human nature to please — that thieves count on to make this scheme work. A form of social engineering — that is, psychological tricks that perpetrators of fraud use to coax targets into turning over money or data — phishing and business email compromise (BEC) are two of the most common forms of business fraud, resulting in nearly $2.7 billion in losses each year.

> **14**
> The average number of malicious emails that employees receive each year.

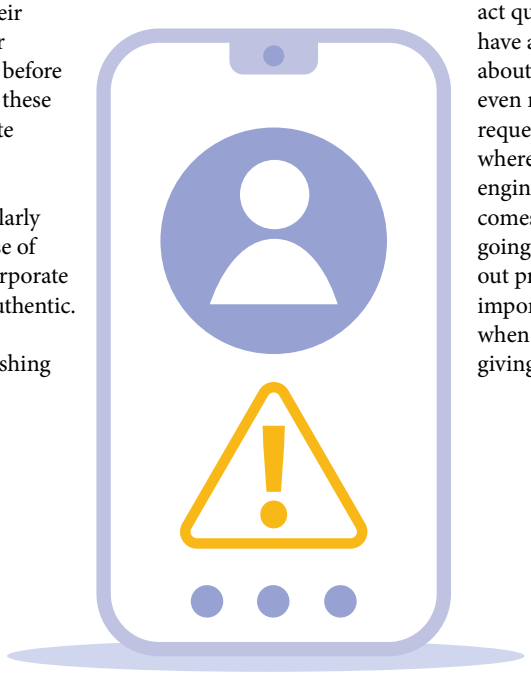
How do these schemes work? According to the FBI, there are multiple forms of phishing/BEC, but typically they involve impersonation — a thief pretending to be someone they're not to gain trust and compel email recipients to expose sensitive information.

In one scenario, a thief might send what's known as a spoof email to someone within a company, changing a small detail in the sending email address to make it seem as though the message is from a trusted source — for example, creating a fake email account that is different by one letter. To someone zipping through their inbox over lunch or clearing out emails before leaving for the day, these seemingly legitimate messages can seem unremarkable and innocuous, particularly when they make use of stolen logos and corporate branding to look authentic.

Perpetrators of phishing and BEC rely on the inattention of their recipients to carry out their fraudulent activities, which generally involve asking for account verification — requiring the recipient to disclose sensitive data like account numbers and payment information — or demanding payment for outstanding invoices and prompting the recipient to pay through a link within the spoofed email. In more sophisticated instances of this scam, the link may take the employee to a website that is identical to the official one, where payment is rendered. Nearly always, these funds are permanently lost.

Another common tactic in phishing/BEC cases involves the impersonation not of a company but of a specific person. Often, it's one of the target recipient's superiors, in a scam known as executive phishing. For example, an employee might receive an email purporting to be from their boss, Jane, who needs them to quickly send them funds (sometimes in the form of gift cards or a wire transfer) or sensitive information (a W-2 form, for example, or a corporate account number). In the latter case, the emailer might say they're off site today and can't access the system, or that they've lost their login and are locked out of a program they need. But always, the message is clear: Act now.

That's not by accident; the urgency is part of the ruse. The employee is pressured to act quickly, before they have a chance to think about how unusual or even nonsensical the request is. That's also where the social engineering aspect comes in: Are you really going to refuse to carry out pressing and important directions when it's your boss giving them?



THE SOLUTIONS

Counteracting phishing and BEC takes a strong commitment to educating employees about the tactics used to carry these schemes out—and a firm-wide pledge never to go around secure channels by, say, emailing about business from a personal address or asking for sensitive data to be sent to you directly. Teach employees to slow down when looking at any email that asks for data or money, because it's better to lose a moment to closer inspection than thousands of dollars to a thief. Finally, show your staff how to spot the signs that an email is spoofed or that the sender has nefarious intent:

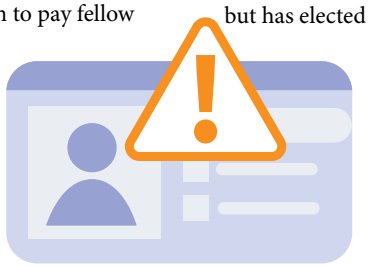
- Does the tone of the email seem odd? Has this vendor or the real Jane ever spoken to you like this before? (If not, it's a clear sign that something is wrong.)
- Is the grammar or diction incorrect? (Errors are a well-known hallmark of phishing emails.)
- Does the link embedded in the email list contain the correct domain name? (If you hover your mouse over it and the preview address isn't what you expect, don't click.)
- Have you ever received a request like this before? If, for example, you've never been involved in paying invoices to vendors or Jane has never requested a wire transfer to her corporate account, that's a strong indicator of something fishy (or, well, phishy).

However, education isn't the only defense against the financial fallout of phishing and BEC. Having a fraud prevention solution in place like Wintrust's Positive Pay offering, which acts as another failsafe — helping ensure that fraudulent checks aren't written and cleared — can spell the difference between a close call and thousands of dollars lost.

SCHEME NO. 2

Check alteration and ACH fraud

The paper check is a hard habit to break, a remnant of an era before digital banking and rapid, easy online transfers. Yet 81% of businesses still use paper checks at least some of the time, most often to pay fellow businesses.



That invites ample opportunity for fraudulent activity, Jaffe explains. "It's just so easy to alter a check," he says. "We have these great, sophisticated financial systems, and here we have a piece of paper clearing through with a name and a dollar amount written on it."

The American Bankers Association reports that upwards of $1 billion worth of fraudulent checks and money orders are recovered each year. In fact, checks are the form of payment most susceptible to tampering and alteration. According to the 2023 AFP Payments Fraud and Control Report, 63% of organizations fell victim to check fraud in 2022.

As Jaffe indicates, there are numerous means by which a check can be tampered with or falsified, but these cases always have one feature in common: somehow, the thief got a hold of a legitimate check, a photograph of one, or simply the information the check contains.

"Every person that a company has ever written a check to has their routing number and account number," Jaffe says. "It's on the bottom of every single check. That information is completely non-confidential. So, the more checks you write, the more you're going to be vulnerable to fraud."

A check can wind up in the wrong hands in a variety of ways:

- An existing check can be stolen from your business' ledger if it's left in an unsafe location that's accessible to unauthorized personnel.
- An existing check can be stolen by an employee who is authorized to use your business' checkbook — someone who has been trusted with sensitive information but has elected to abuse that trust.
- A legitimately written check can be intercepted by a thief, often via the mail.

Once the thief has the check in hand (or, at the very least, the information it contains), they can proceed in a few different ways. Often a stolen check is physically altered via a process called "washing," which involves using chemicals to remove the ink from the check so the thief can insert their own name on the payee line or change the amount to be paid. Other times, an existing check is intercepted by a thief and counterfeited, which involves recreating your business's check using sophisticated printing processes on ink and paper.

Meanwhile, Automated Clearing House (ACH) payments — a digital payment method that sends or withdraws funds to and from individual accounts — are also potential magnets for fraudulent activity. These payments are originated by financial institutions and executed by ACH operators. The popularity of ACH payments has risen steadily each year over the last decade, and 30% of businesses fall victim to ACH debit fraud in 2022.

The most common scenario involves a thief obtaining an organization's bank account information and using it to initiate a fraudulent transfer. Here's where ACH fraud can overlap with previously discussed forms of fraud, such as phishing: a thief can manipulate an employee via email to turn over account or payment information, then use that sensitive info to initiate a transfer. Typically, the company that falls victim to such an attack is liable for the losses.

THE SOLUTIONS

Many check alteration and ACH scams can be thwarted before they start, simply by adopting more diligent security measures. Start by instituting a policy that greatly limits the number of employees who have access to the business' paper checks and sensitive financial information, and require this shortlist of staffers to use two-factor authentication to enter any secure or privileged portals. These moves can greatly reduce the possibility of information landing in the wrong hands.

The mail is often at the root of check alteration scams. In conjunction with the American Banking Association, the United States Postal Inspection Service offers helpful tips for safeguarding checks sent via the mail, including:

- Being more cautious about where mail is deposited and how long it's allowed to sit in plain view before being sent or retrieved
- Following up with payees to ensure that your checks have been received
- Using indelible black ink when writing checks to make check washing more difficult

Often simple solutions can often be the most effective — and tend to be among the most overlooked. "When I talk to a lot of the businesses that have a check fraud claim," Olsen says, "I ask them about their security protocols. How do they think checks got stolen? Do they have a lock on the door? Are there cleaning people allowed to go into that area? Can any employee go in there?"

As Olsen notes, a "clean desk" policy can be hugely effective in the fight against check theft. "Here at the bank, we have a clean desk policy that says I can be written up and even fired if I have sensitive information left on my desk when I leave," he explains. "Businesses should have a mindset that while we can and should assume positive intent in those around us, we should also take precautions."

How Wintrust's anti-fraud solutions work, step by step

A look at how Wintrust's innovative solutions thwart check altering and ACH fraud schemes for Wintrust customers every day — and how they can do the same for your business.

WHAT IS POSITIVE PAY?

This best-in-class feature ensures that thieves can't create or alter a check in your business' name by detecting potentially fraudulent activity before any money leaves your account. Customers upload info about the checks they write, the program compares it to checks submitted for payment, then flags any discrepancies it notes in check amounts, recipients, dates or numbers. These flags are sent to the customer, who approves or denies each payment.

WHAT IS ACH POSITIVE PAY?

The same program as Positive Pay, but for ACH payments. Scan in your authorized ACH transfers and the program will alert you to any unauthorized entries, which you can approve or deny.

WHAT IS REVERSE POSITIVE PAY?

A variation on the original, this feature offers the benefits of Positive Pay, without the manual upload from the business. Instead of uploading the business' check register, the bank simply provides all the checks that have cleared at the end of each day. The client then must meet a daily decision deadline to hold any payments before they are released.

Fraud prevention at work

Paper checks

1. A check is submitted for payment that does not correspond to any of the checks manually uploaded to a customer's Positive Pay account. In this case, while the check numbers are the same, the payee's name and amount are different.
2. An exception is raised by the Positive Pay system and is sent to your queue for approval by the program's daily deadline.
3. You look at the suspicious check, compare it to your accounts, and realize it's an attempted fraud. You deny the payment by the daily decision deadline.
4. You rest easy knowing that nothing is getting past the elite anti-fraud safeguards your business has in place.

ACH transfers

1. An ACH payment is submitted for payment, but the vendor requesting funds isn't on your approved list of payees.
2. An exception is raised by the program, sending you the information about the unexpected transfer so you can decide how to proceed.
3. You realize this is simply a new vendor who hasn't been added to your list of verified payees and decide to approve the payment.
4. That vendor is now added automatically to your list of trusted payees, taking one less task off your plate.

SCHEME NO. 3

Malware and ransomware

As with phishing and spoofed emails, digital fraud schemes often use social engineering to deliver their payload: software that can invade a computer or IT system to steal sensitive data, or in the case of ransomware, hold that system hostage until a ransom is paid.

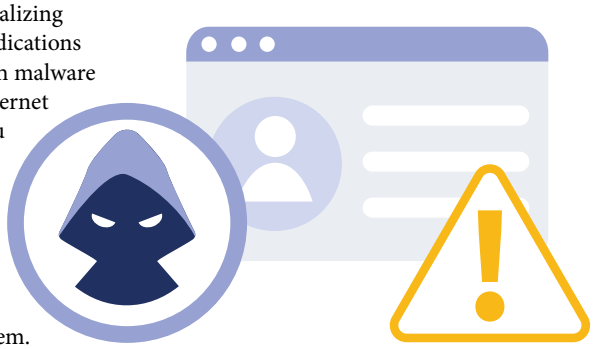
These kinds of attacks aren't about some computer whiz cracking the system, but rather of manipulated employees voluntarily offering up a company's most privileged data. Often, the businesses targeted are relatively small: 46% of cybersecurity breaches impact companies with fewer than 1,000 employees.

> **60%**
> The percentage of small businesses that are forced to fold within six months of a cyberattack.

Malware and ransomware attacks can unfold in different ways:

- **Spyware via attachment:** A phishing email is sent that contains an attachment. When the attachment is opened or downloaded, software is installed on the user's computer that can spy on that person's activities, such as when they enter their credentials to gain access to sensitive data.
- **Spyware via link:** A phishing email is sent that contains a link to a web site. When visited, the site installs malware on the user's computer, infecting it with spying capabilities and keystroke detectors that send sensitive information to the fraud's perpetrators.
- **Ransomware via email:** A phishing email is sent with a link or attachment that, when opened or clicked, installs software that encrypts system data and demands a ransom to restore access to the rightful users.
- **Scareware:** A phishing email is sent that claims a person's computer has been infected with a virus, prompting the recipient to click a link to down load a virus protection program, which is itself the very malware the recipient tried to protect themselves against.

Though ransomware attacks by design involve the victim knowing they've been attacked so they can pay out the ransom, many forms of malware are designed to function without the victim ever realizing they've been targeted. Common indications that a system has been infected with malware include slow performance, your internet browser redirecting you to sites you didn't intend to visit, constant pop-up ads and issues with starting up and shutting down your computer. If you spot these signs, it may be time to pursue an IT solution that can wipe these nefarious programs from your system.



THE SOLUTIONS

The best defense against cyberattacks is the very same defense used to thwart phishing, check alteration and other social engineering scams: education and a strong financial fail-safe. Keep your guard up, don't trust or engage with unusual emails, and make sure your staff know to do the same.

But it's also vital that businesses plan for the worst. There's no banking software that can prevent cyberattacks from finding victims. But if malware is successfully installed within your business' system, programs like Positive Pay or ACH Positive Pay can put a stop to any attempts to turn stolen data or keystrokes into fraudulent payments.

TAKEAWAY

While it's clear that no business can ever be entirely insulated from the threat of fraud, it's equally clear that taking a few simple steps — like educating employees, instituting more shrewd security policies and deploying smart software solutions like Positive Pay — can make all the difference in who remains unscathed and who falls victim. For many businesses, the margin between continued success and potential disaster is increasingly thin. To protect your company's wealth in the long term, you need to remain alert to potential fraud and diligently ensure that you're protected against it.

The expert advice in this white paper was provided by **Ezra Jaffe** (left), Executive Vice President of Treasury Management, and **Ray Olsen**, Senior Vice President of Fraud Management

Connect with Wintrust's Commercial Banking Team