Staying Ahead of Common Fraud Schemes: Understanding and Preventing Fraud

October 28, 2025

Fraud Statistics for 2024

Pinnacle FINANCIAL PARTNERS

2024 Global Financial Crime Report by Nasdaq

- Payments fraud $102.6 billion
- Actual amount could be: $158.0 billion

Fraud Facts

- 95% of cyberattacks are caused by human error
- 67% of cyber-related fraud losses were caused by business email compromise
- 70% of US CFOs say limited controls, risks to liquidity, and payment fraud are challenges for their finance teams
- Individuals in their 20s are experiencing more check fraud than other age groups.

Check Fraud Fun Fact

According to FinCen's latest Financial Trend Analysis, FinCen found three primary outcomes after checks were stolen from the US Mail:

- 44% were altered then deposited
- 26% were used as templates to create counterfeit checks
- 20% were fraudulently signed and deposited

Check Fraud

Pinnacle FINANCIAL PARTNERS

Best Practices

- Positive Pay with Payee Match
- Use Secure Checks
- Pay employees through direct deposit instead of checks
- Secure your check stock
- Move paper payments to ACH or card
- Take checks inside the Post Office to mail
- Always send any high dollar checks by trackable shipping methods if they must be sent via check

AFP Key Findings

Fraud is down very slightly — but remains elevated.

A full 79% of respondents say that their organizations experienced actual or attempted payments fraud in 2024, down slightly from 80% in 2023. The one-percentage-point drop is not very encouraging; 65% of corporate practitioners reported payments fraud at their organizations in 2022. Clearly, fraudsters have not been deterred by any of the anti-fraud protections that organizations have put in place.

Business email compromise (BEC) continues to be a threat.

BEC once again was the number one avenue for attempted and actual payments fraud in 2024, cited by 63% of respondents. Incidence of vendor imposter fraud was also high, at 45%, a sharp increase from 34% in the previous survey. It's important to note that vendor imposter fraud is another form of BEC, as is invoice fraud which increased to 24% in 2024 from 14% in 2023. Spoof emails are still the most prevalent type of BEC, cited by 79% of respondents (up from 77% in 2023).

Check fraud remains constant.

Checks continue to be the payment method most often subjected to payments fraud, with 63% of respondents experiencing attempted or actual fraud via checks in 2024. While that percentage is down slightly from 65% in the previous survey, it is clear that checks remain easy targets for criminals. Nevertheless, more than 75% of organizations currently have no plans to reduce check usage in the next two years.

Wire transfers reclaim their BEC crown.

Wire transfers reclaimed their rank as the payment method most frequently targeted by BEC scammers in 2024, reported by 63% of respondents, up from 39% in the previous survey. Nevertheless, ACH credits — which were the prime targets for BEC in 2023 — were the source of more BEC scam activity in 2024 than in the previous year, rising to 50% from 47%. ACH debits and checks tied for third place at 26% (up from 20% and 18%, respectively).

Classic BEC scams may be falling off.

One significant change seen in this year's survey is the decline in "classic" BEC scams. These are cases in which a fraudster impersonates a senior executive and requests a transfer of funds. In 2023, this method of payments fraud was on par with vendor impersonation, cited by 57% of organizations. In 2024, however, the incidence declined to 49%. Vendor impersonation experienced a slight increase — cited by 60% of respondents — while third-party impersonation remained the most frequent type of BEC scam at 63%. This change in tactics is likely to due to organizations' growing awareness of such "classic" BEC attempts.

Recovering losses has mixed success.

Twenty-two percent of organizations were able to recover 75% or more of the funds lost due to payments fraud in 2024. That is a sharp decrease from results reported for 2023, during which 41% of companies recouped the same amount. However, it is encouraging that the percentage of organizations that were unable to recover anything at all in 2024 was 20%, down from 30% in 2023, and 58% were able to recoup up to 75% of their funds in 2024 (up from 29% in 2023).

Business Email Compromise

- Business Email Compromise (BEC) is a financially-driven cyber threat where criminals target existing business relationships.
- These attackers impersonate trusted contacts or organizations to manipulate victims into making unauthorized financial transfers.
- Perpetrators may alter legitimate invoices or create convincing forgeries.
- In some cases, these scams involve the actual compromise of email accounts to increase authenticity and effectiveness of the fraudulent communications.
- Typically requests for wire transfer, bank account change, request for confidential data or provide a link to click on.
- Create a false crisis or urgency around payments making victims more likely to respond without due diligence.

Business Email Compromise

Pinnacle FINANCIAL PARTNERS

Best Practices

- Always create your own customers, supplier and payee profiles
- Validate all change request you receive independently with your known and established contact
- Consider a “safe word” with your trading partners
- Train staff to spot unexpected invoices or unusual payment request
- Regularly review internal controls and procedures so they are updated to fit your firm’s workflows
- Send a small value test transaction to the new account and confirm receipt with the legitimate beneficiary when sending electronic payments
- Slow down – If an urgent request comes in, follow all internal controls prior to sending payments.

ACH Fraud

Scenario:
A client received an email from their vendor requesting their bank information to be changed. Client handed the change to their accounts payable representative and told them to go ahead and make the change and send a payment of $38K via ACH to their vendor.

Result:
The receiving bank reached out to Pinnacle and asked to verify the transaction with the client because the account number did not match the intended recipient. Pinnacle reached out to the employee that submitted the payment, and the employee said they were comfortable with the payment and the banking change because they received the updated instructions from their vendor via email. Pinnacle highly recommended that the client verbally call the vendor using the phone number they had in their system.

ACH Fraud

What were the red flags?

- A bank account change request
- Change request via email
- The receiving bank called and questioned

ACH Fraud

Best Practices for Prevention or Mitigation

- Verbally calling the vendor at the phone number you have in your system
- Have detailed policies and procedures in place for all employees to follow to confirm any payment change requests
- Train your employees to identify the red flags
- Provide detailed actions to take when employees have concerns
- Know your vendors
- Safe word or phrase with trading partners

Wire Fraud

Client logged into Pinnacle's Online Banking and was prompted to enter her token code upon logging in. She entered her code. Then proceeded to the wire module to input her wire. Before she was finished with her wire, she was prompted again to enter her token code. Client thought it was very odd to be asked for the token prior to clicking "submit" on the wire payment but proceeded anyway. Within a few minutes the client receives an automated alert that wire for $700K had been processed. This was not the wire she had attempted to send!

Wire Fraud

What were the red flags?

- Being prompted to enter token code at odd times during the wire initiation process.
- The thought that something was odd – gut feeling

Wire Fraud

Pinnacle FINANCIAL PARTNERS

Best Practices for Prevention or Mitigation

- Be aware of the links you click on in emails
- Trust your gut!
- Call the bank immediately when your process seems odd and abnormal
- Train employees to identify the red flags
- Provide detail actions to take when they have a concern
- Slow down. If the situation feels rushed, take a step back to regroup

AI Fraud

Pinnacle FINANCIAL PARTNERS

You may have heard this one……

In 2023, an employee in Hong Kong joined a video conference with his company's CFO – only it was not actually his CFO on the call. Scammers had used AI to create a deepfake video of the executive, and during the call, they tricked the employee into transferring $25 million to a fraudulent account.

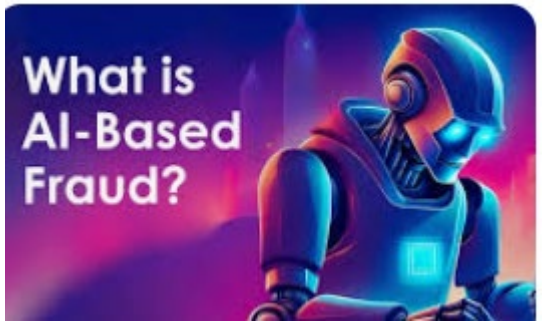
Deepfakes leverage trust: the victim sees a familiar face or hears a familiar voice, so alarms do not go off. These scams also rely on urgency and secrecy (e.g., 'I need this wire transfer now—do not tell anyone'). When we combine emotional manipulation with visual/auditory realism, it is no wonder that even professionals have been fooled. The employee in the $25 million case noticed something odd—the call ended abruptly, and he never directly interacted with colleagues—but only realized it was a scam after the money was gone.

AI Fraud

Pinnacle FINANCIAL PARTNERS

Cybercriminals are using generative AI tools to clone voices and create deepfakes.

AI requires less than 3 seconds of audio to clone a voice. These types of tools are used to trick family members or even bank employees into transferring funds out of the victim's account.



AI Fraud

AI is being used for enumeration attacks. If you have avenues of running transactions online, speak to your merchant provider about ways to avoid this type of activity. There are some settings that can be implemented/adjusted to detect for this type of fraud. Fraudsters use AI to generate primary account numbers and test them consistently through merchant's online channels. They use AI bots to repeatedly attempt to submit online transactions through combination of the primary account numbers, CVV and expiration dates until they get an approval response.

AI Fraud

Pinnacle FINANCIAL PARTNERS

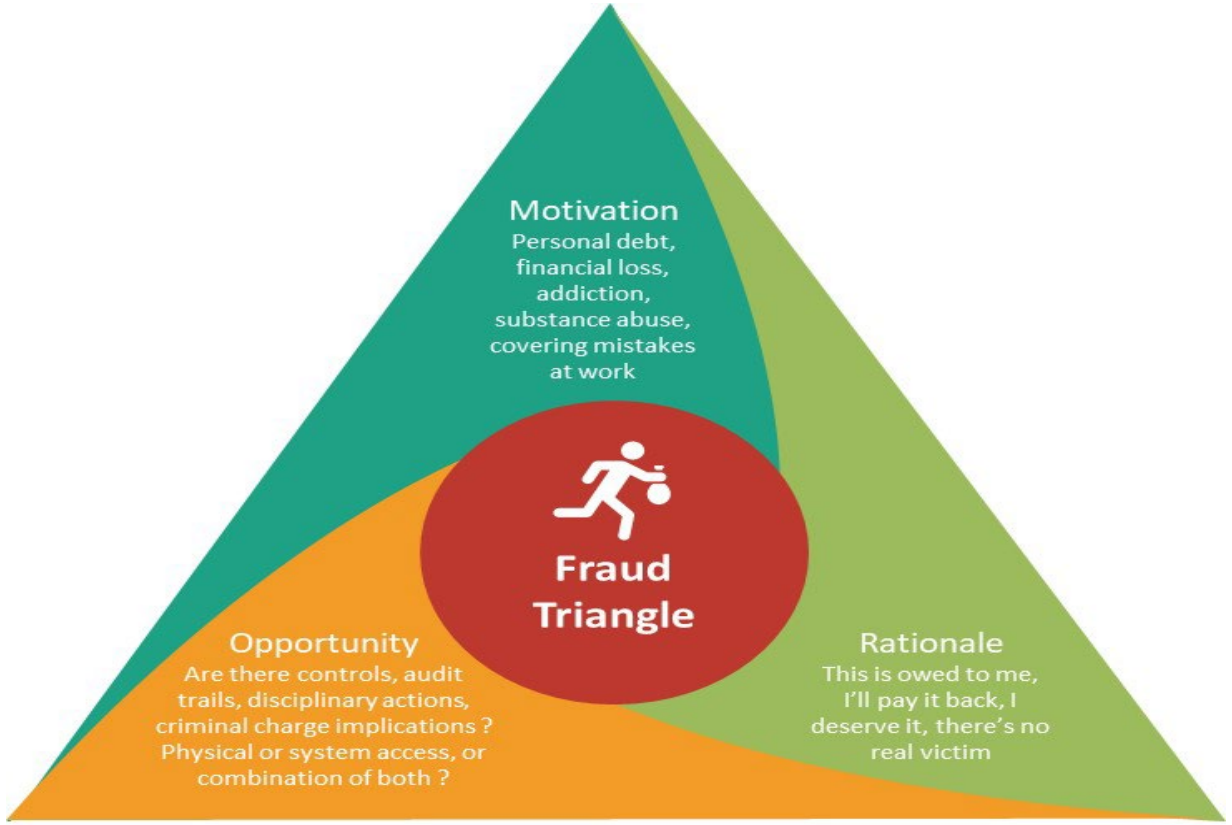
Red Flags & Tools

- While deepfakes can be very realistic, they are not always perfect. There are telltale signs—if you know what to look for. In videos, watch the facial movements and lighting: does the person blink naturally? Do their facial expressions and lip-sync match the audio perfectly?
- Listen for unnatural intonation or odd audio artifacts in voices—a slight robotic timbre or strange pauses could indicate a synthesized voice.
- Most importantly, consider the context: Is this request or scenario unusual? For example, would your boss really demand a transfer over a video call without any prior notice?
- On the tech side, researchers and companies are developing deepfake detection tools—some browsers and email providers are starting to flag suspect media. But these tools are not yet widespread or foolproof.

Why do People Steal??.... Because they can!

Understanding Why People Commit Fraud

Most root causes of fraud can be traced to some combination of motivation, rationale and opportunity.



Why do People Steal??.... Because they can!

Examples Internal fraud

- Fraudulent invoices and purchase orders
- Payroll
- Benefit abuse (PTO)
- Change of account detail requests
- Misappropriation of cash

Why do People Steal??....Because they can!

Pinnacle FINANCIAL PARTNERS

Red Flags

- A colleague displaying an abuse of position or asking employees to circumvent procedures
- Questionable close relationships between staff and vendors
- Any employee or manager refusing to take vacations
- Reluctance to share work duties
- Changes in behavior such as increased defensiveness

Why do People Steal??.... Because they can!

Pinnacle FINANCIAL PARTNERS

Best Practices for Prevention or Mitigation

- Evaluate and Establish strong internal controls.
- Dual Control/Segregation of Duties (i.e., Wire initiator should have separate approver. Vendor management should be handled separate from Accounts Payable, employee responsible for uploading positive pay files should not also have access to decision exceptions, etc.)
- Audit or have oversight over individuals or departments that control money.
- Audit vendors and accounts payable information.
- Frequently monitor aged receivables.
- Ransomware – Plan for these events. You don't want to figure out what to do when it happens, proactively plan in the event your company is hit with an attack. You will need to hire a firm to assist through this process. Interview these companies now so that you know who you would use if this unfortunate event happens. Time is of the essence in getting your business back online.

Ransomware Attack Planning

Pinnacle FINANCIAL PARTNERS

- Internal meeting of department or area heads to discuss plan of action in the event of Ransomware attack.
- Interview and select firms to be used in the event of an attack. When events happen, the company is “dead in the water” until systems are restored. Time is of the essence so the better prepared you are, the better you can react and work under pressure. You may also get better pricing if negotiated up front instead of while under attack.
- There will be no systems access, possibly wi-fi or email access, be ready to continue business without these items.
- Have back up laptops for vital staff and ensure they have internet access at home/cell phones to be able to get back online. Perhaps email provider used has web option so that you can communicate with staff and clients/customers/vendors.
- All internal files should be backed up frequently so you can restore to a point in time if needed.
- Have a list of website favorites saved in files that can be accessed to continue web-based functions such as online banking. Staff get used to using the shortcuts to access systems but don’t know how to get to these sites manually if needed. If victim of ransomware, you will need to know how to get to these sites manually.

Ransomware Attack Planning

- In the planning phase, make the decision of will you rebuild or pay the ransom? Do a cost analysis of rebuilding vs. ransom amount. Decide what ransom amount is too much.
- Work to change any passwords for all applications. Actively keep a list of these applications/websites so you know all applications/websites that need credential changes in the event of an attack.
- Do you have a Cyber Crime related insurance policy? If not, review if you should get one. Ensure terms are favorable. If not, these are negotiable. Add any to policies/terms if insufficient.
- If you have Cyber crime insurance, understand the terms and ensure these are followed if an event were to happen to ensure policy will pay if an event.
- These types of criminals are typically “honest” criminals. Once the ransom is paid, your files are restored.
- The aftermath… Ensure great policies and procedures are put in place to avoid an additional attack.

Best Practices for all Fraud

- Positive Pay with Payee Match
- ACH Filter and/or Blocks
- Reconcilement- daily if possible
- Email notifications, text and limit alerts
- Dual control on all payment methods
- Strong password
- Written Internal policies and procedures
- Safe word
- Listen to your gut

Questions

Pinnacle FINANCIAL PARTNERS