WELLS FARGO

Cyber payments fraud and risk



November 5, 2026

Stephen Lenehan, Relationship Manager
Lynn Nieves, Treasury Management Consultant
Jackie Kobialko, Treasury Management Consultant

© 2026 Wells Fargo & Company.

Agenda

- Current fraud landscape
- New and evolving threats
- Social engineering
- Business email compromise
- Account takeover
- Artificial intelligence-enabled fraud
- Critical strategies your organization needs for fraud protection
- Fraud education resources



Current fraud landscape

It only takes one incident for your organization to be compromised. The impact can be significant.

76% of organizations faced actual or attempted fraud in 2025[1]

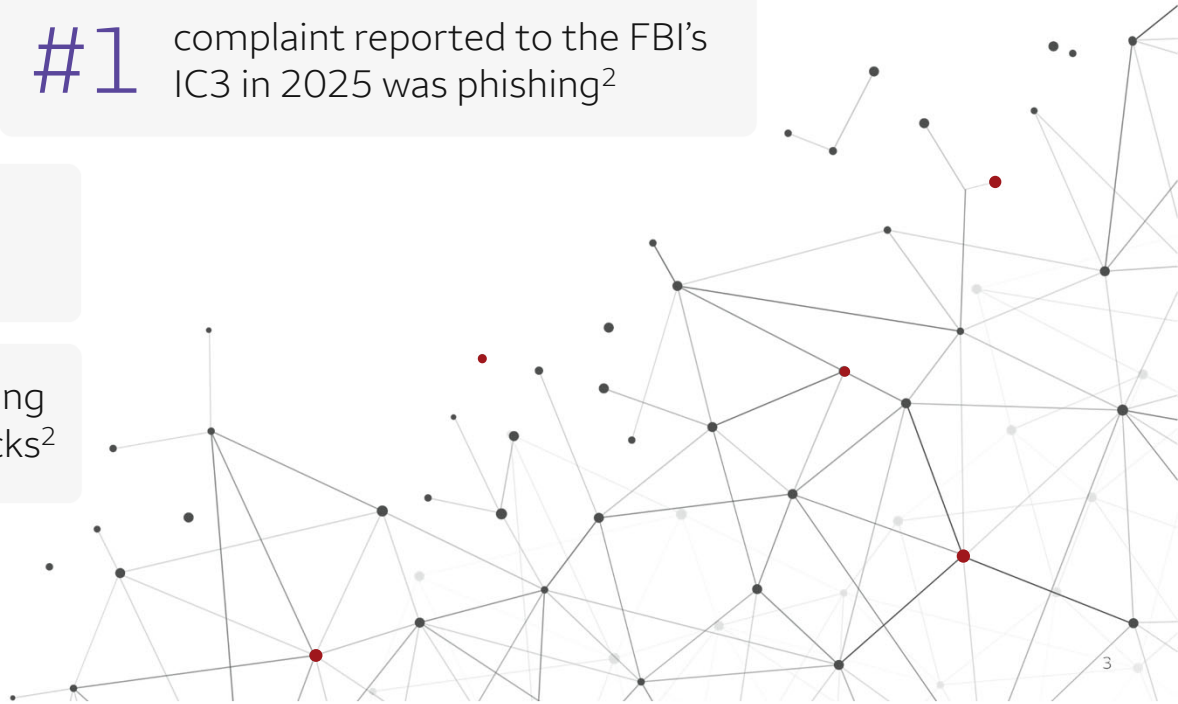
#1 method most vulnerable to fraud attempts in 2025[1] was check payment

$10.2M average cost of a data breach in the U.S.[2]

#1 complaint reported to the FBI's IC3 in 2025 was phishing[2]

$3.0B total losses from business email compromise reported in 2025[3]

1 in 6 number of data breaches reporting in 2025 involving AI-driven attacks[2]



1. Association for Financial Professionals, 2026 AFP® Payments Fraud and Control Survey Report
2. IBM, Cost of a Data Breach 2025 Report
3. Federal Bureau of Investigation, 2025 Internet Crime Complaint Center Internet Crime Annual Report

Current fraud threat landscape

Business email compromise (BEC) aka **imposter fraud**

Fraudsters impersonate a vendor, company executive, or another trusted trading partner — ultimately tricking you into making the payment to them.



Account takeover (ATO)

Thieves gain access to bank accounts and make unauthorized transactions by stealing portal login credentials.

What are you doing to reduce your exposure?



Fraud scenarios

Scenario 1: Senior Executive impersonation

- Be cautious if you receive a phone call from a senior executive instructing you to initiate a large payment.
- Treat the request as high risk if it:
  - Is **out of pattern**, or
  - Requires **confidentiality**, or
  - Demands **immediate** action
- Do not proceed with sending funds until the request is verified.
- The call may be a fraud attempt using an **AI-generated deepfake voice to impersonate the executive**.
- Always **verify the request by calling the executive back** using contact information from your employee directory or another trusted internal source.

Scenarios are based on actual client incidents



Fraud scenarios

Scenario 2: Vendor impersonation

- Be alert if:
  - You receive an email from a vendor contact requesting a change to payment instructions for an upcoming invoice payment, and
  - Shortly after, you receive a phone call from the same contact to confirm their email.
- **Do not rely on inbound phone calls** for verifications of payment-related requests.
- It may be a **fraudster impersonating the vendor using a deepfake voice**.
- Instead, **always independently verify** all requests by contacting the requestor yourself using **known and trusted** contact information.

Scenarios are based on actual client incidents



Social engineering: understanding the threat

The use of deception to manipulate employees into taking actions that benefit fraudsters — sending payments or revealing sensitive credentials

Attacks target people and processes, not just systems

Two of the most impactful forms:

- Business Email Compromise (BEC)
- Account Takeover (ATO)

Common entry points:

- Emails (phishing)
- Text messages (smishing)
- Phone calls (vishing)
- Fake websites or login pages



98% of cyber attacks start with social engineering*

* Gitnux. Social Engineering Attacks Statistics 2026 Report. Updated May 2026.

Business email compromise (BEC)



BEC is among the most financially damaging online crimes, targeting companies of all sizes by tricking employees into making transfers or revealing sensitive information.

Rather than relying on complex malware, sophisticated criminals invest time and patience conducting research. They then use that insight to exploit trusted relationships and human psychology — feigning urgency, authority, or familiarity — to drive significant losses.

Business email compromise (BEC)

The typical lifecycle of a BEC attack includes:

Reconnaissance

Fraudsters study an organization, monitor employee communications (through hacked accounts), and identify key decision-makers in Accounting, Finance, Treasury, or HR.

Impersonation

They spoof email addresses or fully hijack the accounts of legitimate executives, customers, or vendors.

Manipulation

Attackers craft urgent, authoritative messages that pressure victims to act quickly. Messages include requests for urgent vendor invoice payments, large wire transfers, or sudden changes in payroll direct deposit.

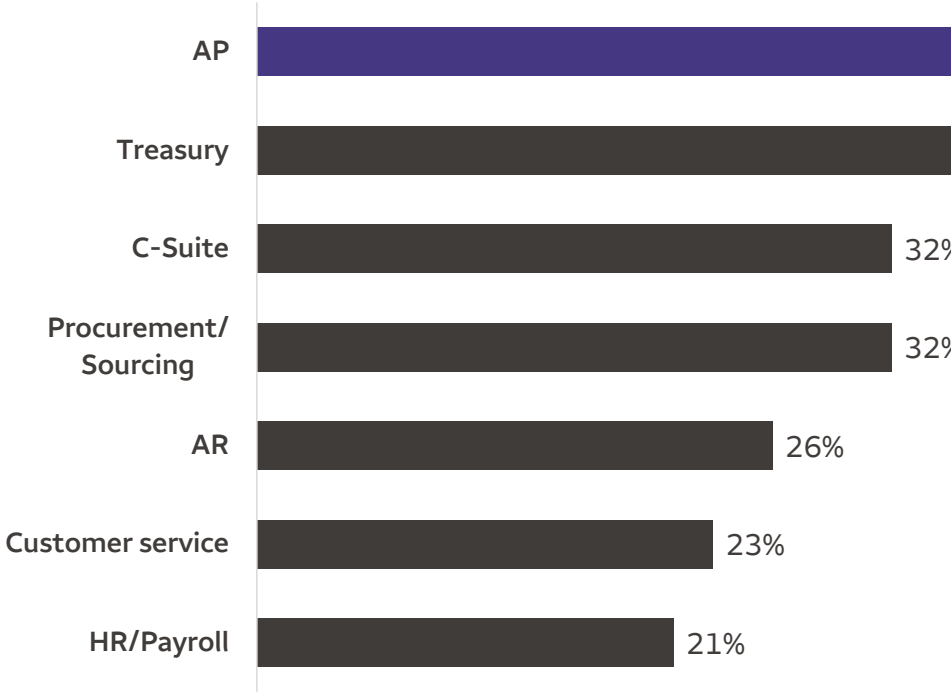


Why attempts are so effective:

- Requests appear legitimate
- Fraudsters exploit urgency and trust
- Attempts leverage real business processes

BEC fraud can occur across your organization

Departments most vulnerable to targeting by imposter scams



Source: Association for Financial Professionals, 2026 AFP® Payments Fraud and Control Survey Report.

Steps to protect against BEC fraud

Verify the request

- Never approve payments based on voice, video, or email alone.
- Watch for red flags, especially if a request is out of pattern.
- Confirm the details of the request.
- Only use the contact information you have in your system of record.

Implement dual custody

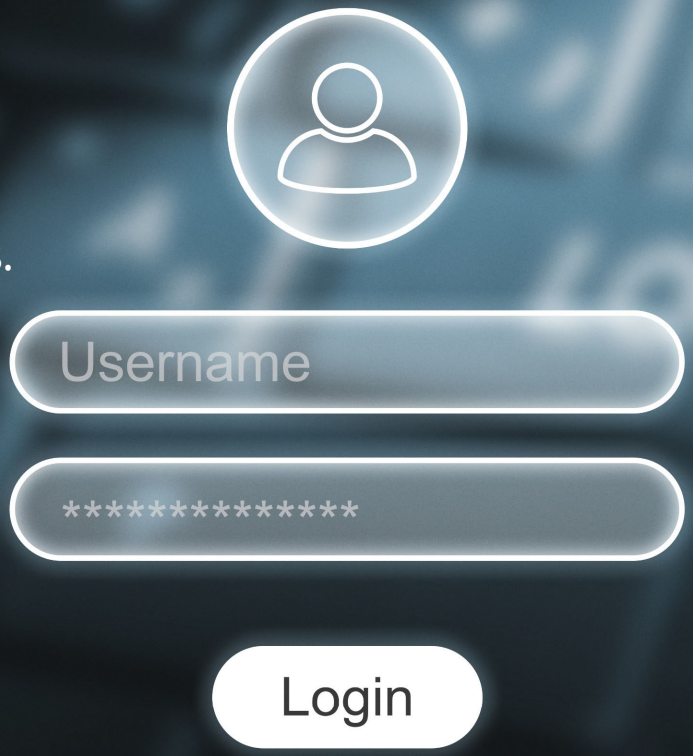
- Require at least two people to initiate and approve transactions or changes.
- Use this process as a second chance to identify potential fraud.

Monitor your accounts

- Reconcile bank accounts daily and pay close attention to account activity.
- Segregate money movement responsibilities.

Account takeover fraud (ATO)

Fraudsters often use **social engineering** or **malware** to steal confidential login information and gain direct access to your online accounts.



Social engineering: tactics (such as phishing) to trick individuals into sharing confidential information

Malware: malicious software that gives criminals access to systems and accounts

Steps to help protect against account takeover fraud

Do

- Use **multi-factor authentication** for accessing your organization's networks and accounts.
- Practice **strong password hygiene —** create complex and unique passwords for each account.
- **Update systems, applications, and security software** promptly and ensure they are current and patched.
- Review employees' **banking portal access and payments entitlements** regularly to ensure they are current.
- Use **alert services** to receive text or email notifications regarding electronic debits from your accounts.

Don't

- **Do not** share online banking credentials.
- **Do not** click on links or download programs or attachments in emails or text messages unless they are from a trusted sender.

Protect your credentials

Be wary of unsolicited phone calls concerning unreported banking portal issues or payment verifications.

Items Wells Fargo will **NEVER** ask for:

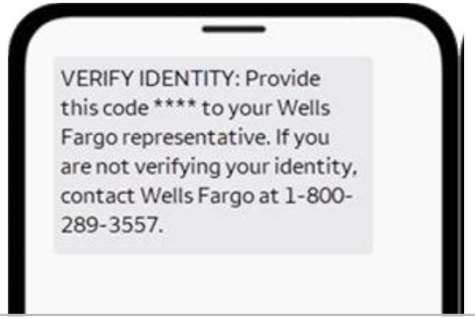
- Wells Fargo Vantage® password
- Token PIN
- PIN + RSA SecurID token code combination (passcode)
- A second user in your organization to join a call and provide their credentials to verify or approve a transaction (in a dual custody situation)
- Secure Validation codes we send you for payment authorization (example below)

Immediately contact your Wells Fargo team if you are asked for this information in an email or phone call



Items Wells Fargo **MAY** ask for:

- First and last name
- User ID (if you contact us)
- Company ID (if you contact us)
- RSA SecurID token code (six-digit code by itself)
- Secure Validation codes we send you to verify your identity (example below)



Screen images simulated

Critical actions you can take now

Consider **your needs**

One size does not always fit all

Your security measures should reflect your organization's priorities.

Consider **your controls**

Assess your procedures

Review processes regularly and adjust as necessary.

Consider **your actions**

Be prepared and ready

Have an incident response plan in place to respond in case of a fraud attack.

Internal control methods and recommended practices

Establish rules and outline responsibilities

ACH fraud

- Procedures outlining vendor validation process for new or updated relationships
- ACH debit controls
- Account validation services
- Daily reconciliation

Check fraud

- Positive pay
- Payee validation
- Daily reconciliation
- Segregation of accounts
- Check block for non-disbursing accounts

Artificial intelligence-enabled fraud

Cybercriminals can leverage AI — generative and agentic — for their schemes in a variety of ways, including:

- **Enhancing the sophistication and realism** of phishing emails and corresponding fake websites, increasing the likelihood that victims will fall for the scams.
- **Automating the process of generating new variants** of malware, making it more challenging for traditional systems to detect and block them effectively.
- **Planning and executing end-to-end fraud campaigns** with agentic AI tools, generating up to 4.5 times more revenue than traditional fraud tactics.

Sources: Abnormal Security: CISO Guide to Generative AI Attacks; Interpol Global Financial Fraud Threat Assessment.

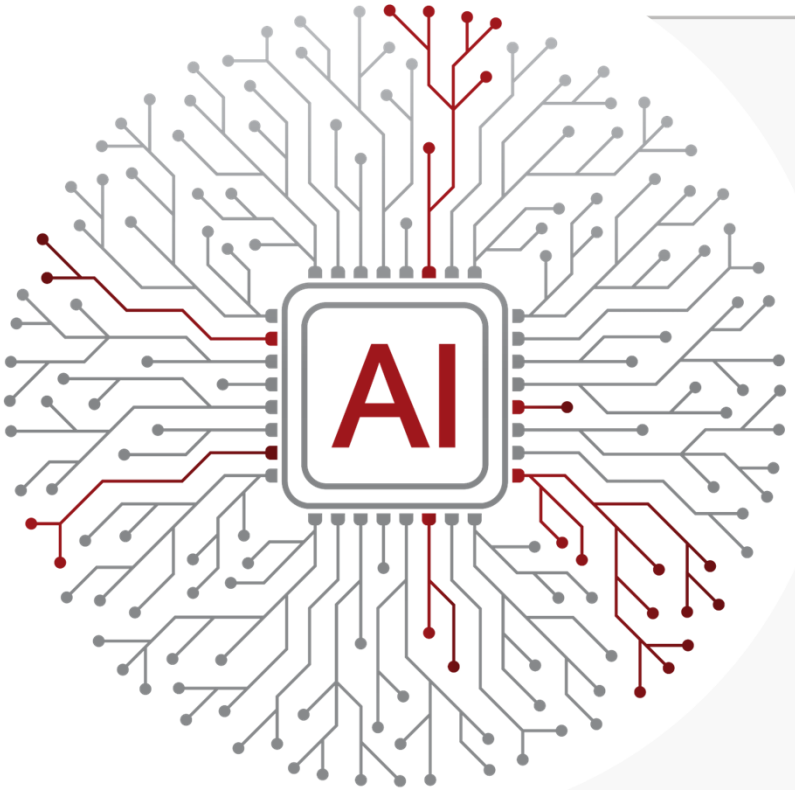


There has been an **89% increase** in AI-enabled cyberattacks

CrowdStrike 2026 Global Threat Report

Generative artificial intelligence

Deepfake voices and images of people you know



AI can also be used to create deepfake voices or facial images — which can sound or look like someone a user knows — to deceive them.

Example

An employee talking to a person they believe is their chief financial officer is more likely to process a fraudulent payment.

Artificial intelligence

How to protect your organization

In-depth defense: Implement a layered defense combining people, process, and technology to help counter evolving AI threats.

Enforce strong verification and approval protocols

- Train employees to challenge realism — never approve payments or changes based on voice, video, or email alone as these may be AI-generated.
- Verify all requests, including those from senior executives, using trusted, pre-established contact information.
- Implement dual custody controls as an additional checkpoint.



Technology considerations

To help block these threats from reaching your employees, experts recommend:

- Deploying AI-driven detection systems
- Using multi-layered detection (behavioral, technical, metadata)
- Implementing continuous control monitoring

Source: Deloitte, Enterprise Security Frameworks

95% of data breaches involve a human element.

SC Media. “95% of data breaches involve human error, report reveals.” March 2025.

Staying safe and protected

Things to consider

Employees are an organization’s **greatest asset** and a **critical line of defense** in protecting it.

Use caution when **discussing your job online** (including on social media and networking sites).

Limit the details provided in your **out-of-office messages**.

Connect securely by **avoiding free, unprotected Wi-Fi**.
Use a VPN to access Wi-Fi in public spaces.

Do not use work devices for personal activities, or allow family members to use them, to help prevent malware infection.

Employee education and awareness to help mitigate the risk

Educate your entire staff



- Create a **security-minded culture** — never trust, always verify.



- Make sure that training is **continuous** and **role-based**.



- Ensure **new employees** are adequately trained on controls and procedures.



- Reinforce training with ongoing **awareness campaigns** and **leadership messaging**.



- **Encourage** and **empower employees** to question payment or account change requests, even from executives.

Third-party due diligence

Vendor and trading partner awareness

Talk to your vendors and trading partners about **their cybersecurity posture** — they are targets for fraud too.

Ensure

they are **taking measures** to protect their information assets.

Consider

sharing your own prevention best practices with them.

Define

a **communication process** for payments-related requests.

Suspect payment fraud? Here is what to do next.

Fraud action items

If you suspect fraud with an electronic payment you have sent, **immediately notify** the following:

- Your dedicated client service officer
- Global Payments & Liquidity Service at **1-800-AT-WELLS** (1-800-289-3557)
- Your relationship manager

Note: Fraud recovery efforts are extremely time- sensitive and are not guaranteed —— the faster you let us know, the better your chances of recovery.

You should also **file a report** with one or more of the following resources for assistance with the fraud:

- FBI Internet Crime Complaint Center website (ic3.gov)
- Local FBI field office
- Local police department

Suggestions

- Notify your own IT and risk management teams of the incident so they can take any necessary remediation measures including identifying other compromised users within your organization.
- Review all recent payments to find other potential fraudulent transactions that may have been processed.
- Analyze the incident to identify any potential gaps in your processes to determine if additional internal fraud controls or employee training are needed.

Note: We encourage you to report all fraud attempts you experience to Wells Fargo — even the ones you were able to stop — as that information can be helpful for us in preventing future fraud.

Fraud recovery process and updates

- Recovery timeframes vary among banks and can take up to 90 business days or longer, depending on the Receiving Depository Financial Institution (RDFI).
- Your assistance with supplying all relevant information promptly, including any required documentation, helps expedite the recovery effort.
- Wells Fargo actively engages with RDFIs on all fraud recoveries. We are dependent on the RDFI and their investigation processes including frequency of updates.
- As we receive information from the RDFI we will relay it to you (if not restricted by privacy regulations).
- Your client service officer or your relationship manager are your primary points of contact for updates on fraud investigations and recoveries.

Resources for additional fraud protection information

Wells Fargo websites

Fraud & Security page
wellsfargo.com/com/fraud

External resources

FBI Internet Crime Complaint Center (IC3)
ic3.gov

Cybersecurity & Infrastructure Security Agency (CISA)
cisa.gov

Note: to use the links, highlight the link, right click and select “Open Hyperlink” – if reading hard copy, enter the https address on your browser.

Q&A



WELLS FARGO

Thank you