WELLS FARGO

Emerging Banking Fraud Risks and Bank Mitigation Tools

Reid Andrews
Edwin Guzman

July 2026

© 2026 Wells Fargo & Company.
Deposit products are offered through Wells Fargo Bank, N.A., Member FDIC. Wells Fargo Bank, N.A. is a banking affiliate of Wells Fargo & Company.
Wells Fargo Bank, N.A. is not liable or responsible for obligations of its affiliates.

Agenda

- Current fraud landscape
- New and evolving threats
- Business email compromise
- Account takeover
- Critical strategies your organization needs for fraud protection
- Q&A

Payments fraud continues to be a significant business risk

It only takes one incident for your organization to be compromised

2025 fraud statistics

Organizations of **all sizes** and **across all industries** are at risk.

While this percentage is down slightly from last year, it remains well above 2022 levels, suggesting that fraudsters remain undeterred by controls organizations have put in place.

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

In 2025, organizations experienced what percentage of fraud by check?

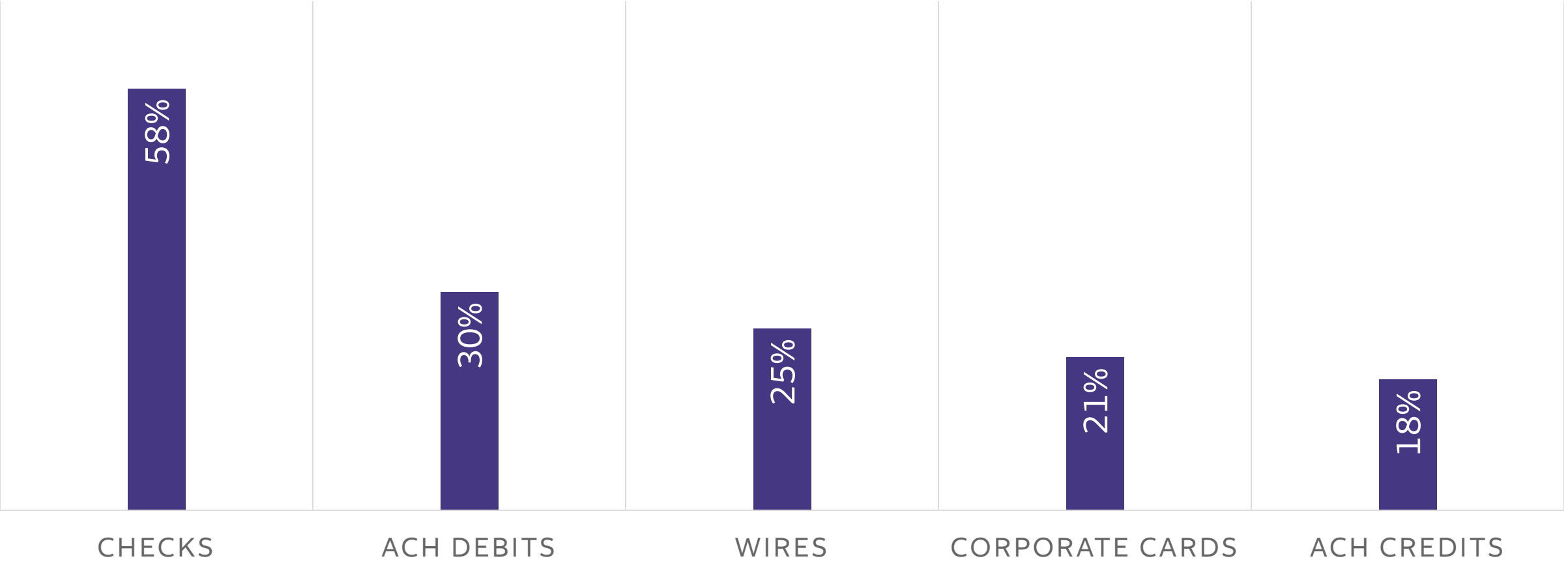
1) 30%

2) 58%

3) 21%

Are your payments a target for fraud?

Payment methods impacted by fraud



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

Current threat landscape

Key fraud threats impacting customer-facing digital channels

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.

Online account takeover (ATO)

Thieves gain access to make unauthorized transactions by stealing banking portal log-in credentials.

Business email compromise (BEC) — aka Imposter fraud

> Business email compromise is one of the most financially damaging online crimes, targeting companies of all sizes by tricking employees into making transfers or revealing sensitive information.

— Federal Bureau of Investigation

Sophisticated fraudsters + time and patience = **significant losses**

How they target you

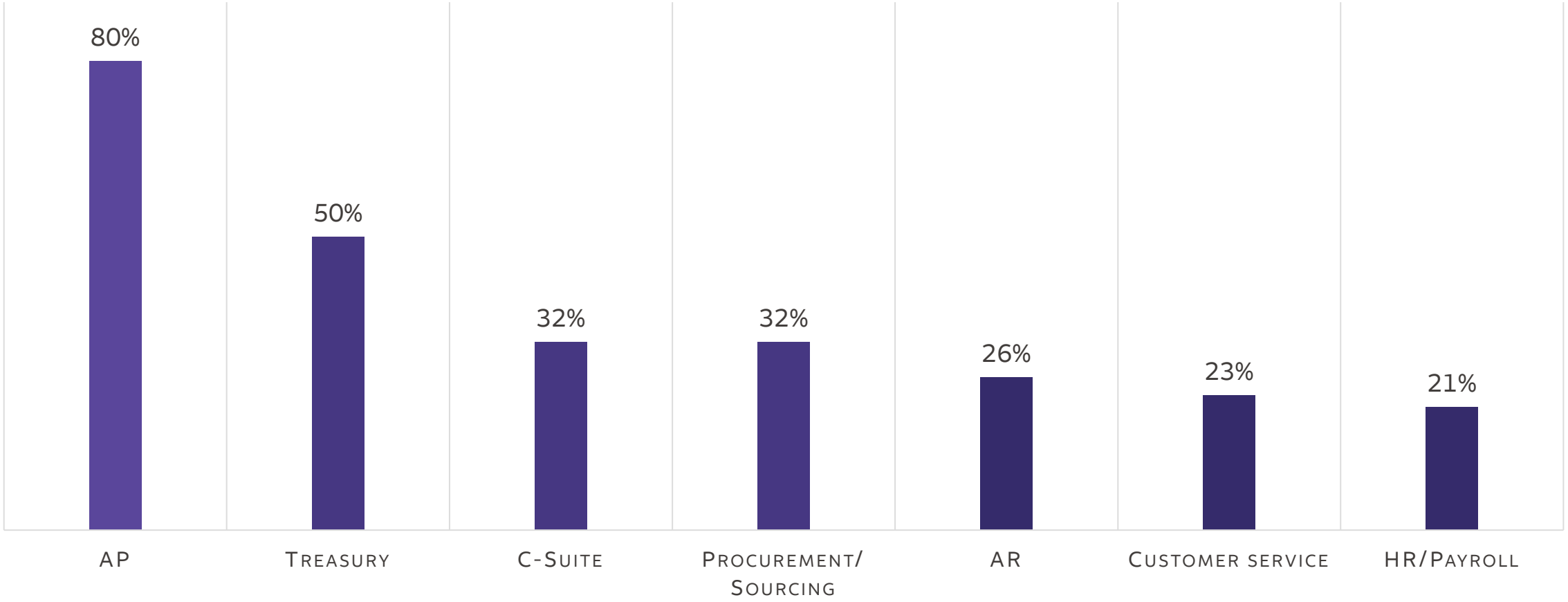
- **Spoofed** email address
- **Compromised** email account

Why it works

- Fraudsters **research targets**
- Attempts **appear legitimate** at first

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 help protect against BEC fraud

Verify the request

- Watch for red flags, especially if a request seems out of the ordinary
- Verbally verify and confirm the request
- Only use the contact information you have in **your** system of record

Implement dual custody

- Serves as a second chance to identify potential fraud
- Verify changes and pay attention to the details before initiating payment
- Confirm changes are verified before approving payment

Monitor your accounts

- Reconcile bank accounts daily and pay close attention to account activity
- Protect your email account and login credentials

Account takeover (ATO)

Theft of confidential information to access online accounts directly

Fraudsters typically leverage **social engineering** and **malware** to execute an account takeover incident

Social engineering

For example, **phishing**, manipulates you into divulging confidential information

Malware

Malicious software is installed on your computer without your consent or knowledge and allows a fraudster to access accounts and **send unauthorized payments**

Steps to help protect against ATO fraud

Do take these steps

- **Use alert services** to receive text or email notifications regarding electronic debits from your accounts
- Implement **dual custody**
- Use **multi-factor authentication** for accessing your organization's networks and accounts
- Keep **antivirus software current** on all devices you use to access your networks
- Install all **system and application updates** for patching security flaws in timely manner
- Review employees' **banking portal access** and **payments entitlements** regularly – to ensure they are current

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're from a trusted sender

Caution

- Be wary of unsolicited phone calls concerning unreported **banking portal issues** or **for payment verifications**

Protect your credentials

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

- Wells Fargo Vantage℠ password
- Token PIN
- PIN + RSA SecurID token code combination (passcode)
- 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

Generative artificial intelligence: Take steps to help manage risk

What you need to know

Cybercriminals can leverage **generative artificial intelligence** for their schemes in a variety of ways, including:

Enhancing

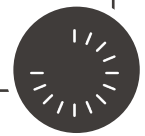
the sophistication and realism of phishing emails and their corresponding fake websites — can increase the likelihood of users revealing sensitive information or inputting credentials.

Building

trust with a target by using specific information about them along with previous conversation history.

Automating

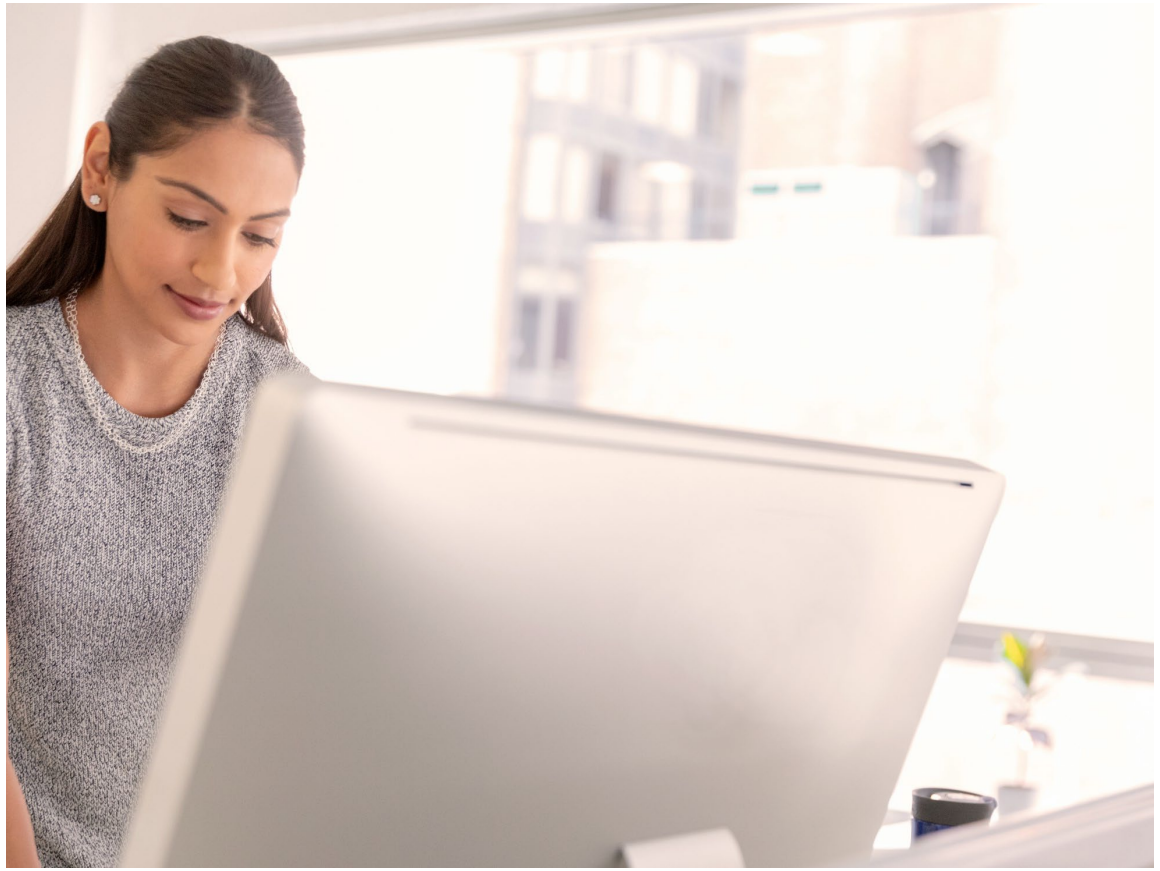
the process of generating new variants of malware — making it more challenging for traditional systems to detect and block them effectively.



Source: Abnormal Security: CISO Guide to Generative AI Attacks

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 that they believe is their chief financial officer is more likely to process a fraudulent payment.

Generative artificial intelligence

How to help protect your organization

Did you know?

According to Gartner – half of organizations lack confidence in traditional email security solutions to detect and block AI-generated email attacks.

Gartner – How to Protect Organizations Against Business Email Compromise Phishing

Counter the threat with best practices

To counter this new threat, it's generally considered an industry best practice to implement AI-based secure email gateway solutions that offer:

- Advanced business email compromise phishing protection
- Behavioral analysis and imposter detection
- Internal email protection

Additional considerations

- Implement robust internal payment verification processes
- Utilize dual custody for payments and user administration
- Train your employees on fraud prevention

Staying safe and protected

Employees are an organization's **greatest asset** — they can also be the **biggest weakness…**

Things to **consider**

Use caution when **discussing your job online** (i.e., 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 your work devices for personal activities — or allow family members to use them — to help prevent malware infection

Education and awareness to help mitigate the risk

60% of working adults are unsure of their responsibilities in securing their organization[1]

Educate your entire staff

- Establish a **regular and ongoing process** for educating staff
- Create a **security-minded culture** — never trust, always verify
- **Instruct and empower all employees** to question all payment or account change requests — even from executives

Vendor and trading **partner awareness**

- Have **ongoing conversations** with your vendors and trading partners about **their cybersecurity posture** — they are targets for fraud, too
- Consider **sharing** your own prevention best practices with them
- Define a **communication process** for payment-related requests

1. 2024 Proofpoint Account Takeover Statistics

Internal control methods for check fraud

Establish rules and outline responsibilities

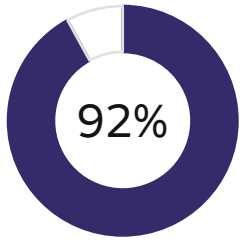
Recommended practices

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

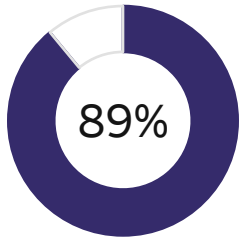
Internal control methods for check fraud

Percentage of organizations **with implemented method**

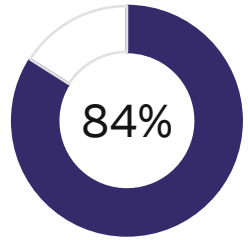
Positive pay



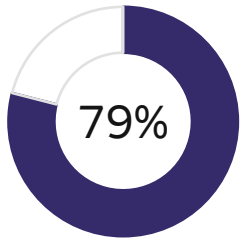
Daily reconciliation



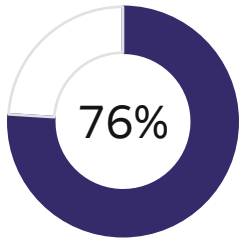
Segregation of accounts



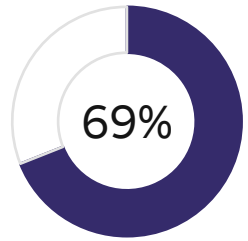
Payee positive pay



Tamper resistance features



“Post no checks” restriction



Source: Association for Financial Professionals, 2023 AFP® Payments Fraud and Control Report

Internal control methods for ACH fraud

Establish rules and outline responsibilities

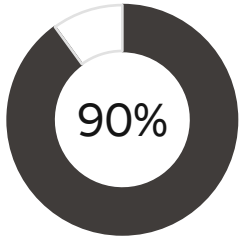
Recommended practices

- Document procedures on vendor validation process for new or updated relationships
- ACH debit controls
- Utilizing account validation services
- Daily reconciliation

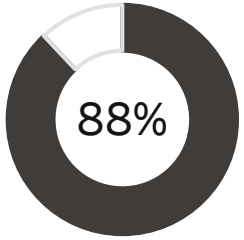
Internal control methods for ACH fraud

Percentage of organizations **with implemented method**

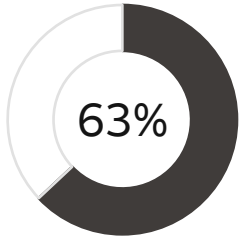
Block all ACH debits except on designated account(s) set up with ACH debit filter



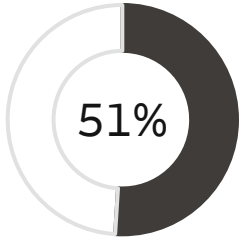
Reconcile accounts daily to identify and return unauthorized ACH debits



Debit block on consumer items, and debit filter on commercial ACH debits

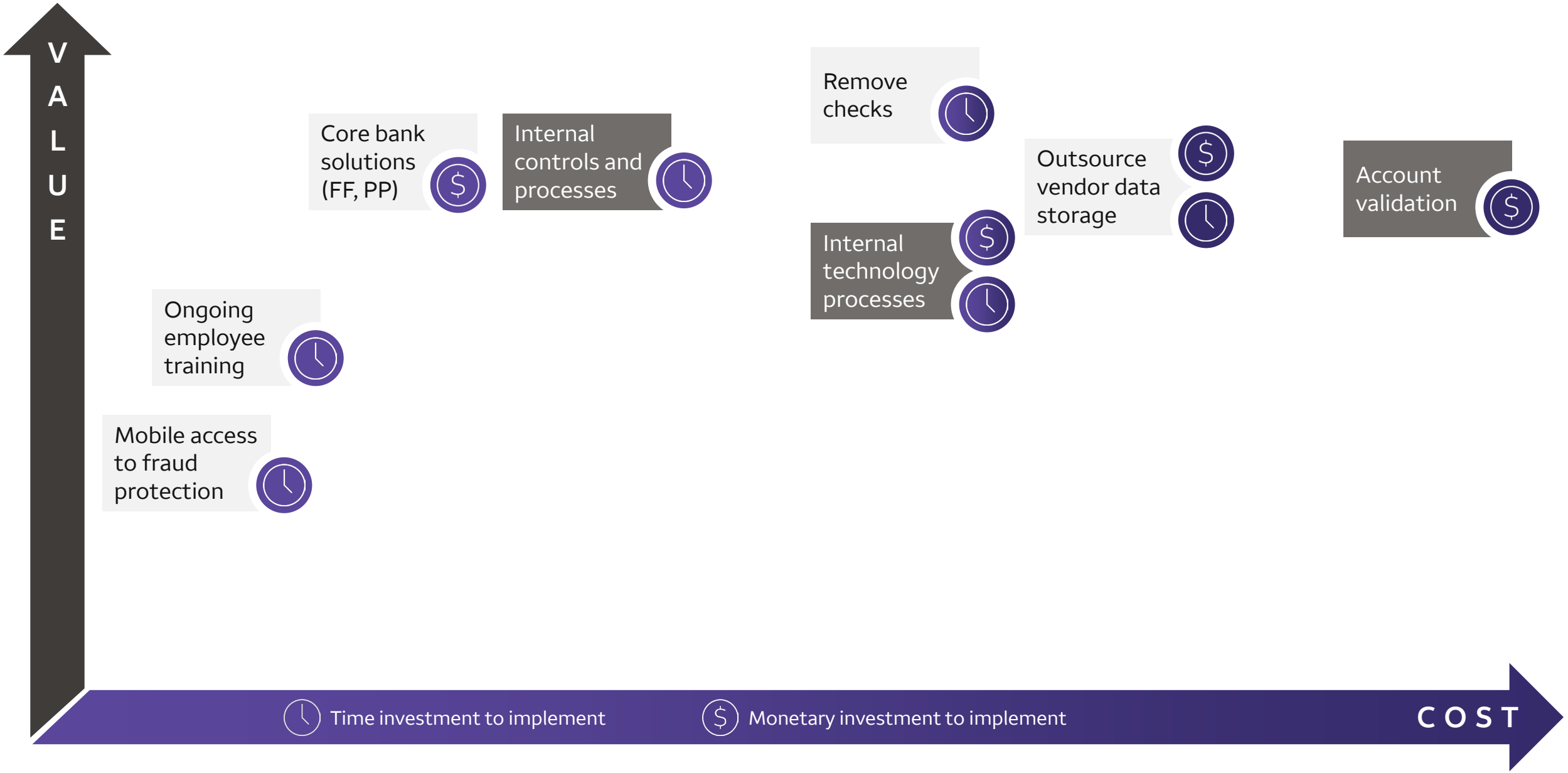


Block ACH debits on accounts



Source: Association for Financial Professionals, 2023 AFP® Payments Fraud and Control Report

High value internal controls to consider



Account validation

What it is

A nationwide database that contains data for **561 million accounts** from participating banks, which are updated nightly after each posting cycle.

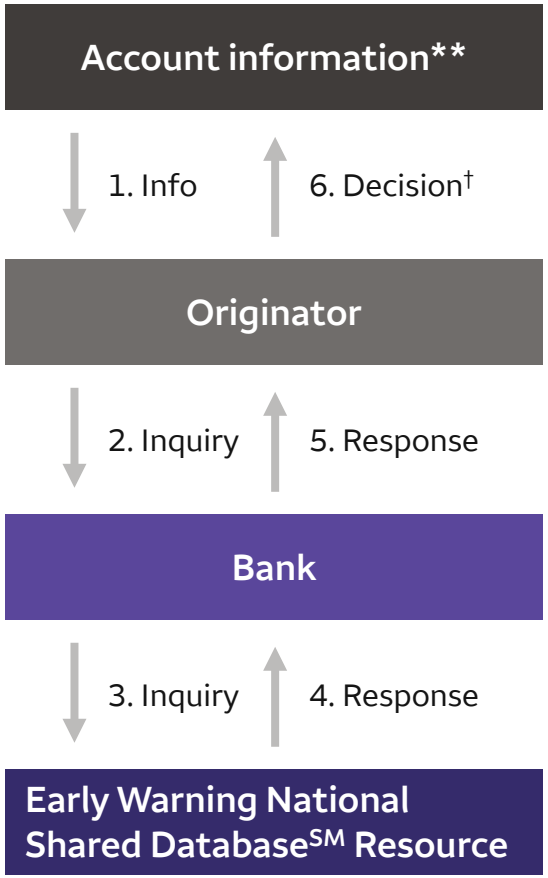
Early Warning Services, LLC

100% bank owned service

- Bank of America
- BB&T
- Capital One
- Chase
- PNC
- U.S. Bank
- Wells Fargo

- **Regulated** by Office of the Comptroller of the Currency and the Consumer Financial Protection Bureau
- **Recognized** as a Specialty Consumer Reporting Agency
- **Processed 11.1 billion** check items for posting, **53.2 million** stop payments, and **47.2 billion** ACH items*

How it works



* Data provided by Early Warning Services, last updated March 2024.
** Account information is submitted by the person or party that wants to make or receive a payment. This could be a customer, consumer, vendor, employee, or counterparty.
† Decision will trigger an action such as pay, don't pay, use different payment information, call customer service, or need more information.

Education and awareness to help mitigate the risk

Patching human vulnerabilities through security **awareness training** is just as important as patching technical vulnerabilities[1]

Educate your entire staff

- **Establish a regular and ongoing process** for educating staff
- **Instruct all staff**, especially AP staff, to question unusual payment or account change requests received by email — even from executives
- **Alert** management and supply chain personnel to the threat

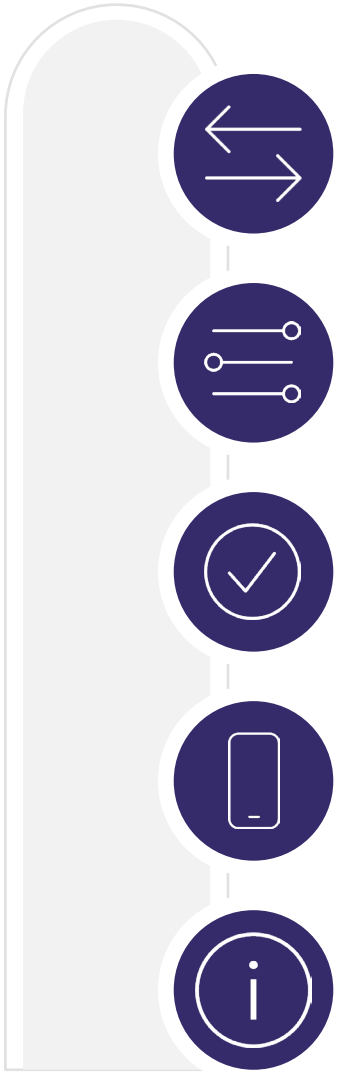
Vendor and trading **partner awareness**

- **Educate your vendors and trading partners**—they are targets for fraud, too
- **Define a communication process** for payment and account changes

Employees must be right **100%** of the time, while threat actors need to be right **only once** – and they know this.[2]

1. 2023 Treasury Perspectives Survey Report, Strategic Treasurer
2. Abnormal Security H1 2023 Email Threat Report

Steps to help protect against payments fraud



Dual approval for high-risk transactions

Positive pay and **ACH fraud filter**

Account validation services

Mobile access to fraud features

Employee **training** and increased **awareness**

Q&A

Resources for additional fraud protection information

Wells Fargo websites

- Wellsfargo.com 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.

WELLS FARGO

Thank you