AFP 2021
IN-PERSON | VIRTUAL

Identify Crises: Best Practices in Fraud Mitigation

Steven Bernstein
Executive Director
Treasury Services
J.P.Morgan

Frank D'Amadeo
Assistant Treasurer
conEdison

Steve Dellasega
Senior Manager
EARLY WARNING™

Executive Summary

Fraud Overview & Current Trends

Digital world creates opportunity, fraudsters are becoming sophisticated, we'll review data points and trends for types of fraud faced today and forms fraud comes in

Fraud Mitigation Tools

Overview of industries best in class tools for fraud mitigation and prevention

Tool Use Cases

Review of real-world applications for fraud mitigation tools and practices

Best Practices & Governance

Beyond tools, we will evaluate industry best practices to mitigate fraud and recap regulation updates

AFP 2021
IN-PERSON | VIRTUAL

Agenda

1. Fraud Overview & Current Trends
2. Fraud Mitigation Tools
3. Tool Use Cases
4. Best Practices & Governance

Rise of Fraud

- Fraudsters are becoming more active, sophisticated and strategic
- Increase in digital world opens opportunity, but threats can be recognized and mitigated

56% Of organizations uncovered fraud after one week and 20% after one-month[1]

71% Of organizations were targets of scams in 2020[1]

56% Of organizations increased use of online treasury tools and electronic payments[2]

Mitigation Steps

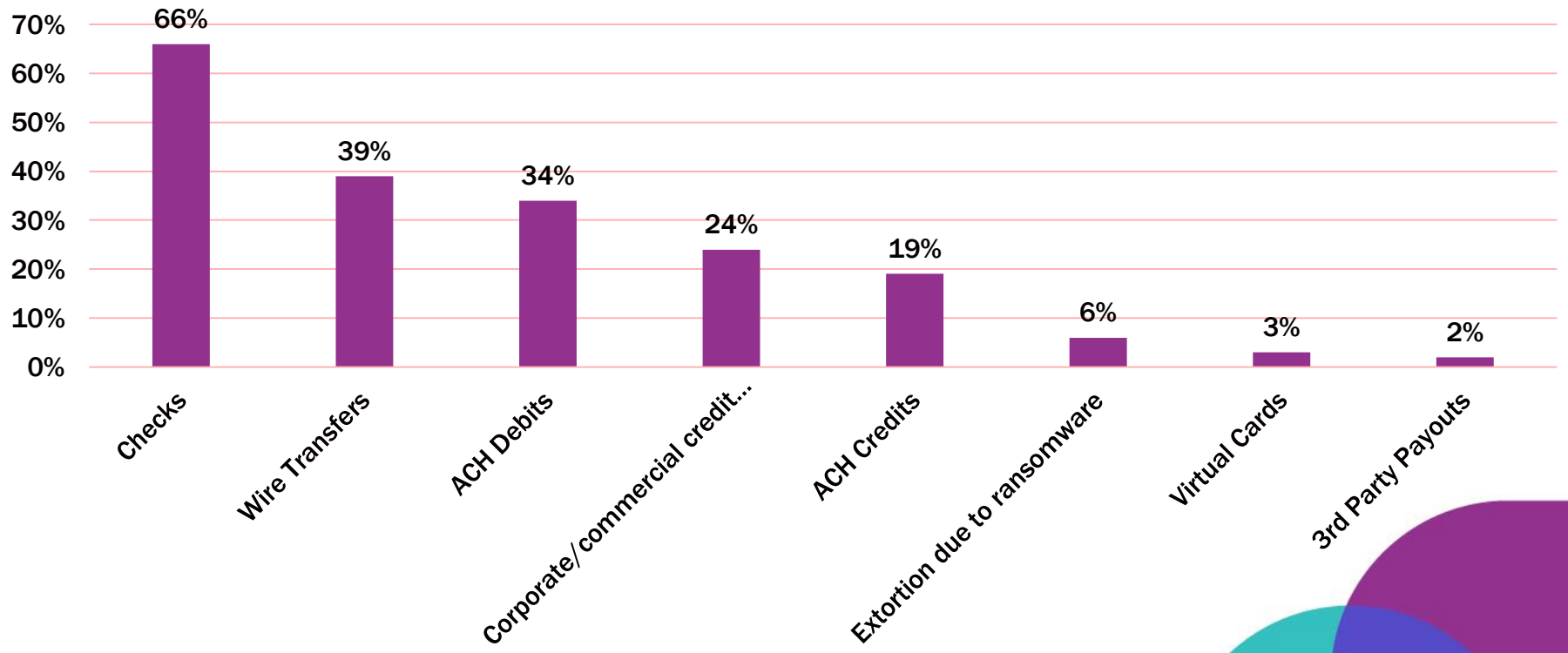
- ❑ Industry Best Practices
- ❑ Tools for Fraud Mitigation
  - ❑ Transaction Reconciliation and Protection
  - ❑ Account Validation Services
- ❑ Tokenization
  - ❑ Ability to identify accounts by tokens allocated
  - ❑ Not relying solely on account numbers

[1]2021 AFP Payments Fraud and Controls Survey

[2]JPMorgan Chase (Business Leaders Outlook, January 2021). JPMorgan Chase's Business Leaders Outlook survey was conducted online from November 11-24, 2020, for small businesses (annual revenues between $100,000 and $20 million) and from November 13 to December 1, 2020, for middle market companies (annual revenues between $20 million and $500 million).

Payment Fraud Trends

Checks, Wire, ACH are leading payment Methods that Were Targets of Attempted and/or Actual Payments Fraud in 2020
(Percent of Organizations)



2021 AFP Payments Fraud and Controls Survey

AFP 2021
IN-PERSON | VIRTUAL

Fraud Comes in Many Forms

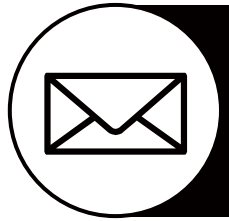
Impersonation of authoritative academic or governmental organizations requesting personal data, soliciting donations to “charities”, or directing targets to fake websites with additional information on health statistics

Increased abuse of a company’s own brands to target that company’s employees with the above strategies

Emails or phone calls inquiring about organizational working arrangements, such as percentage of staff or types of roles working remotely – this information can then be used in future attacks

Overall, payments fraud from third parties continues to increase with 44% of BEC related to vendor impersonation[1]

Bad actors leveraging social media channels asking for personal information or directing targets to malicious websites

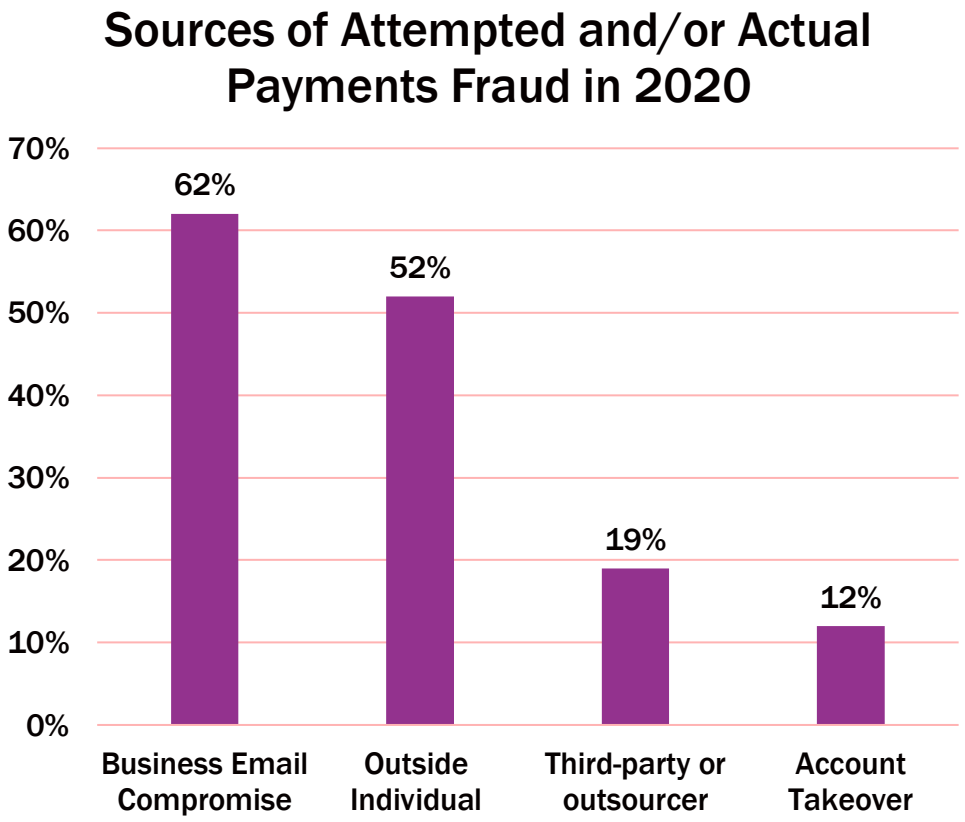


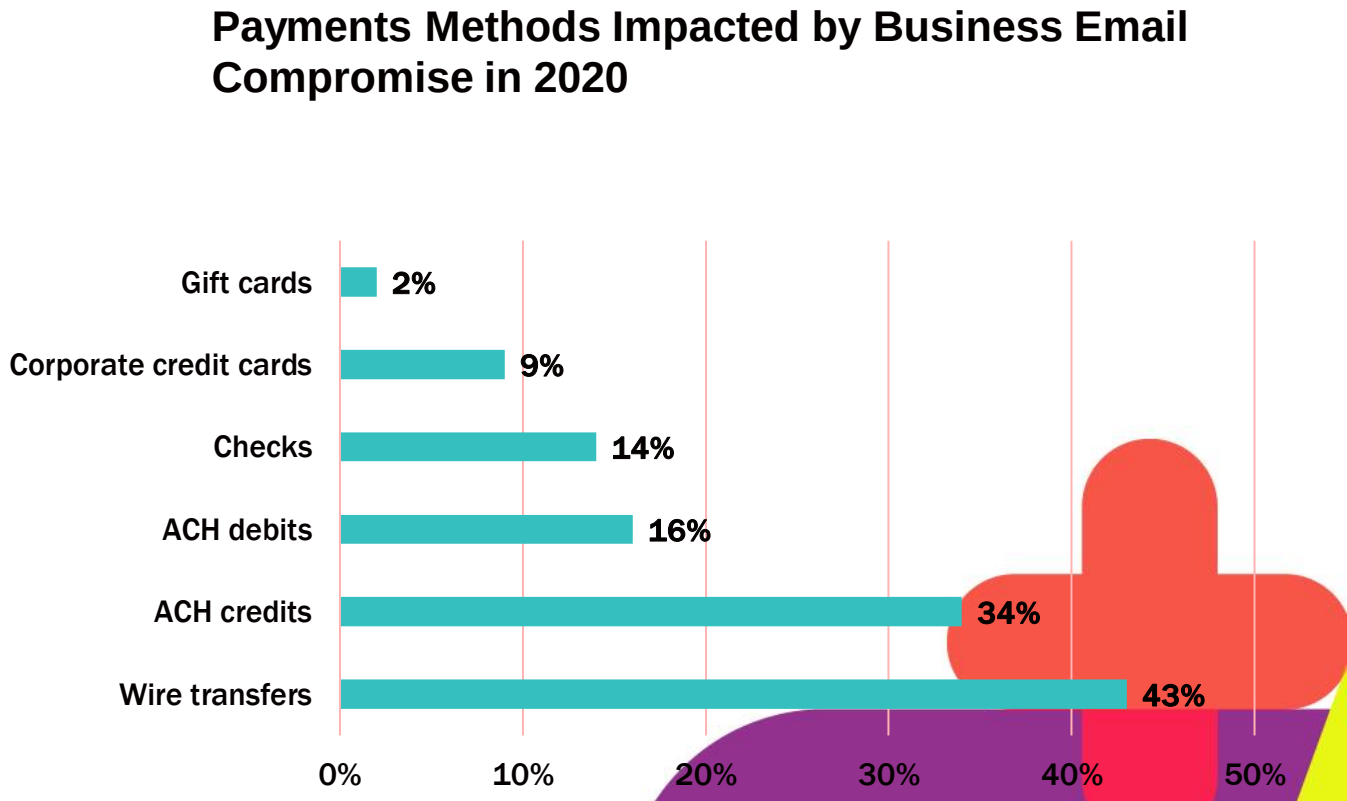
Use of email to deliver financial malware continues to be a dominant attack method with 65% of threat groups using spear-phishing to compromise their victim’s networks and 1 in 412 emails containing malware[2]

Over 75% of companies are adopting stronger internal controls that prohibit initiation of payments based on emails or other, less secure messaging systems[1]

Note: [1] 2021 AFP Payments Fraud and Control Survey Report; [2] 2019 Symantec Internet Security Threat Report; [3] Internal J.P. Morgan data

Payment Fraud Trends - BEC Fraud Leads



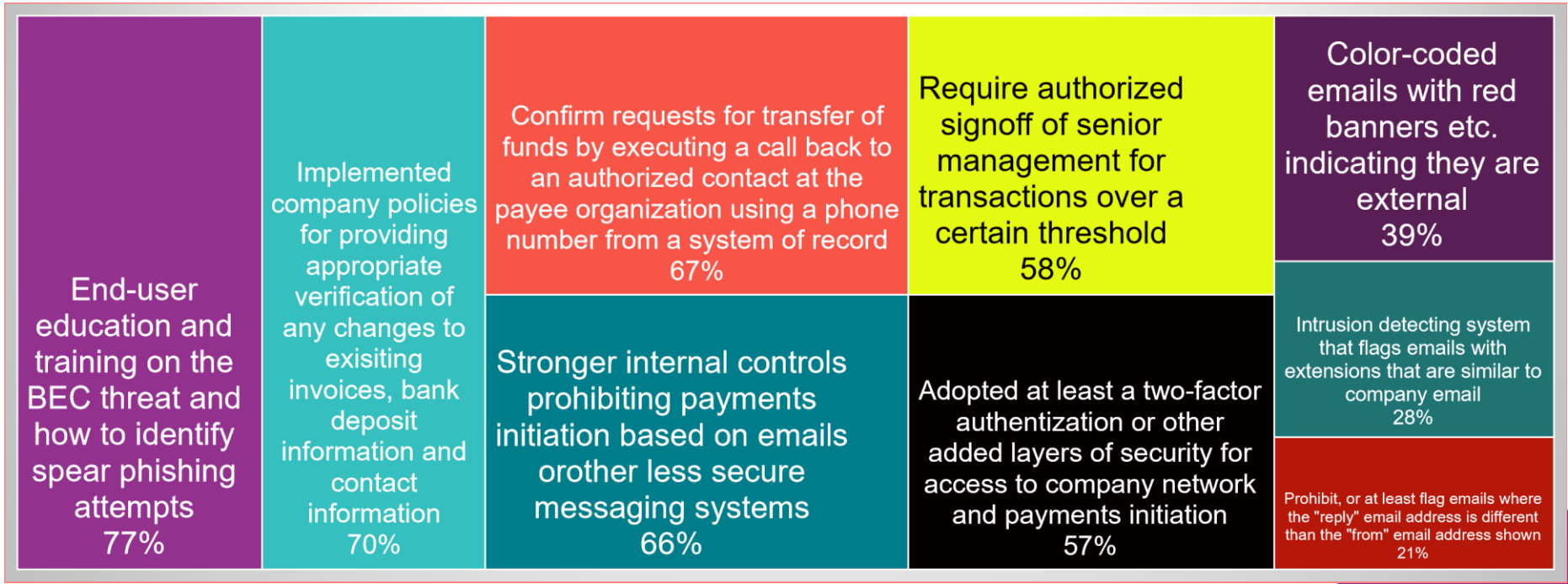


2021 AFP Payments Fraud and Controls Survey

AFP 2021
IN-PERSON | VIRTUAL

Internal Controls for BEC Fraud

Internal Controls Methods Implemented to Prevent BEC Fraud (Percent of Organizations)



2021 AFP Payments Fraud and Controls Survey

AFP 2021
IN-PERSON | VIRTUAL

Agenda

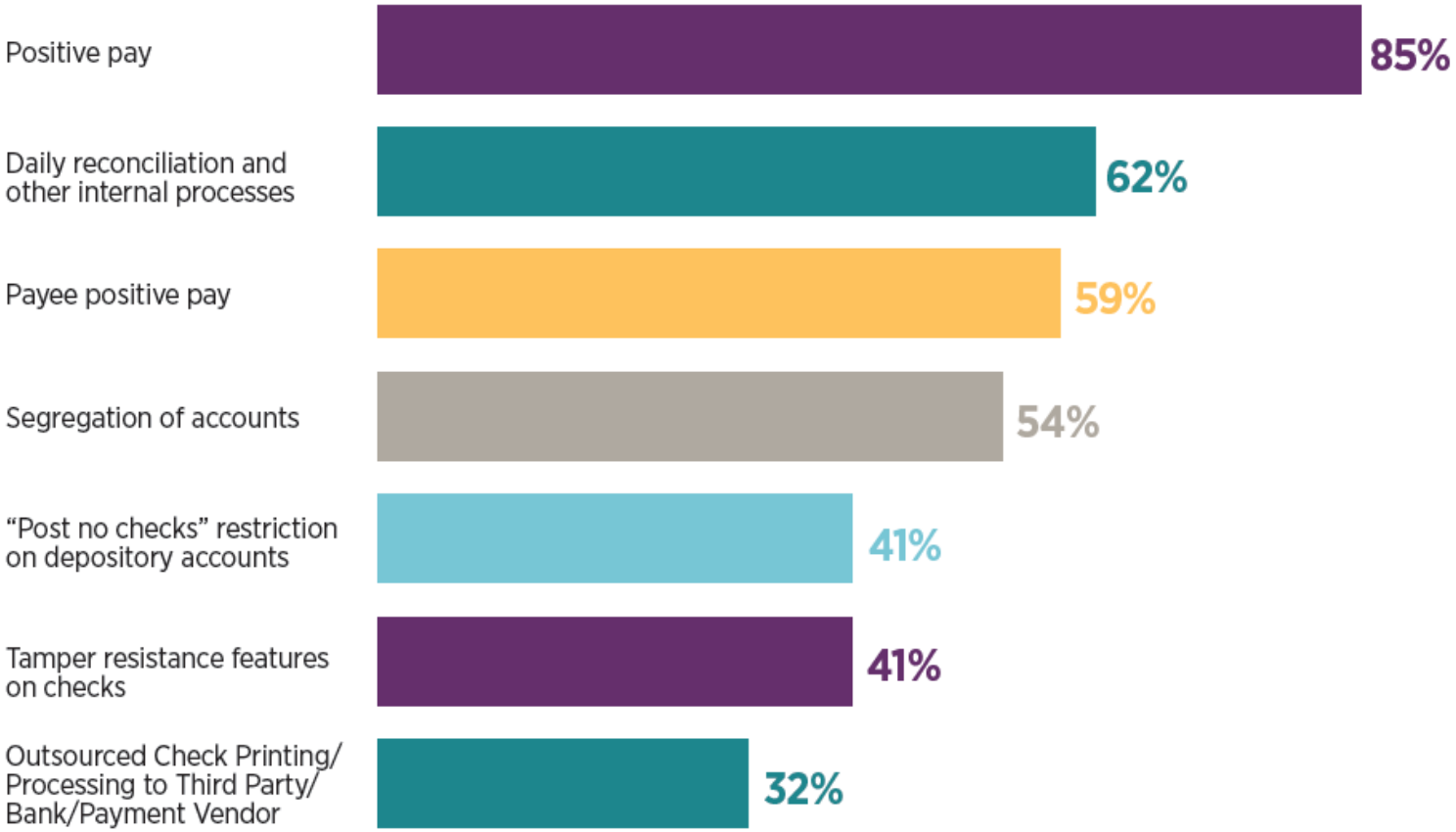
1 Fraud Overview & Current Trends

2 Fraud Mitigation Tools

3 Tool Use Cases

4 Best Practices & Governance

Check Fraud Mitigation Tools Used Today



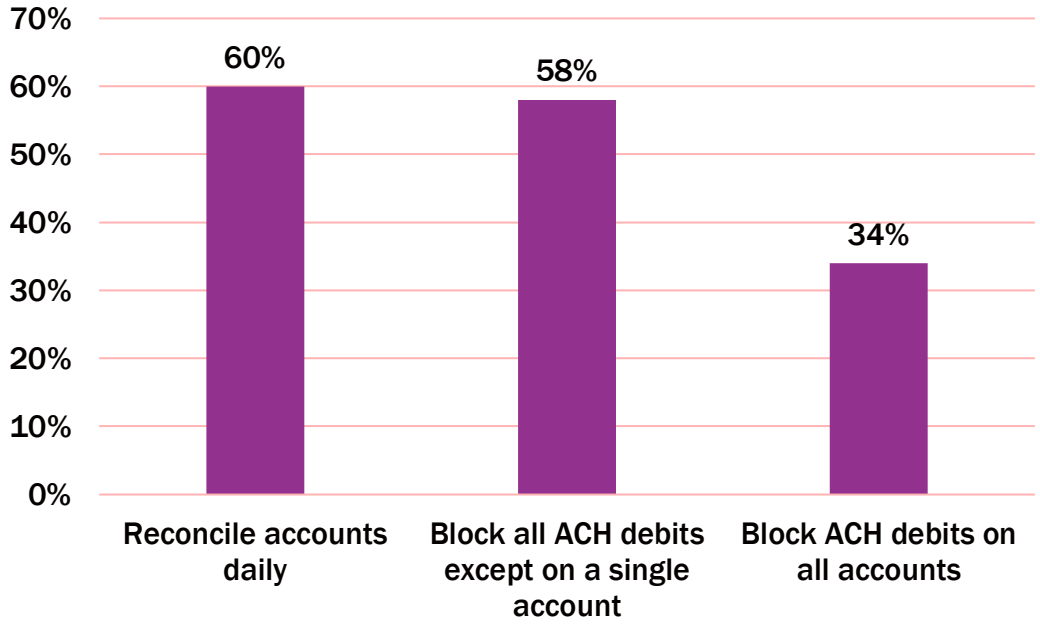
Fraud Control Procedures and Services Used to Protect Against Check Fraud

(Percent of Organizations that Experienced At Least One Attempt of Check Fraud)

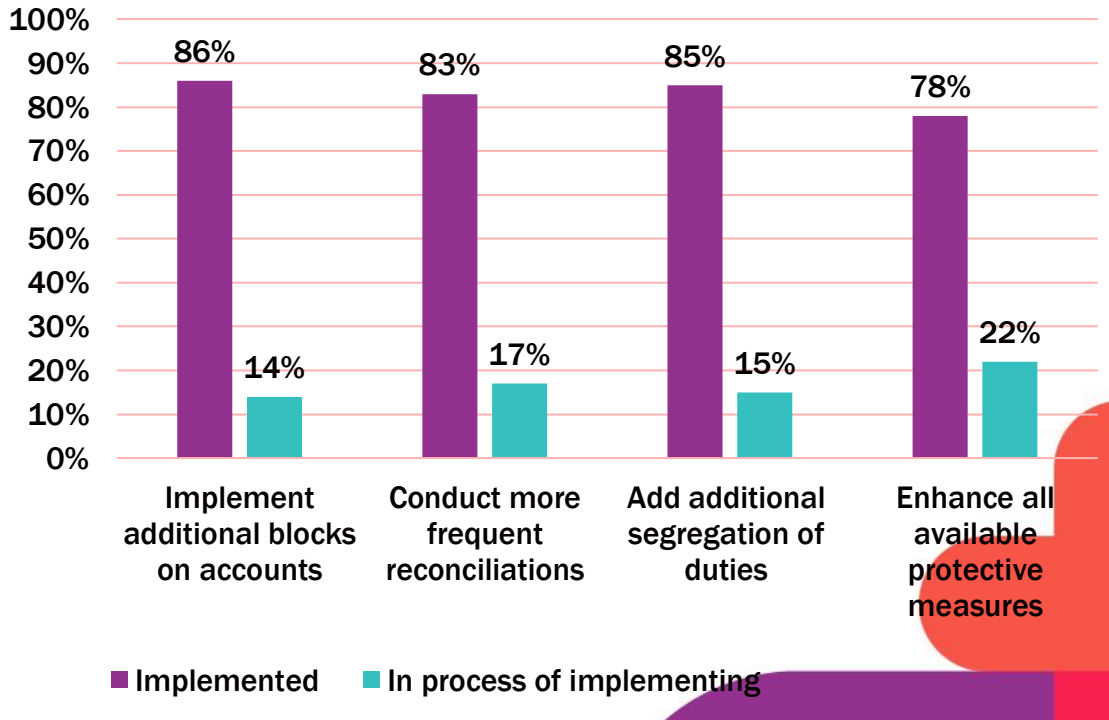
2021 AFP Payments Fraud and Controls Survey

ACH Fraud Mitigation Tools Used Today

Fraud Control Procedures or Services Used to Prevent ACH Debit Fraud



Revisions Implemented/Are Being Implemented to Safeguard Against Fraud



2021 AFP Payments Fraud and Controls Survey

AFP 2021
IN-PERSON | VIRTUAL

Choose the right solution for your business—ACH Security Services

Block or decision BEFORE posting

Transaction Blocking

Automatically block unauthorized ACH debit and credit transactions from posting

TIP: Ideal for when no debits or credits should post

How it works:

- Received ACH debits and credits that match block settings are returned automatically without posting
- No option to review and decision unauthorized ACH activity prior to blocking or posting, which may result in unintended returns and potential related missed payment deadlines and penalties

ACH Positive Pay

Get notified of blocked transactions, change decisions to pay and add allowable IDs for future transaction

TIP: Ideal for ensuring all received ACH debits and credits are authorized, preventing unintended returns and postings

How it works:

- Received ACH debits or credits generate alerts
- Choose to change the Pending Return or Pay decision applied based on the blocking profile

Review and decision AFTER posting

Transaction Review

Review and confirm transactions posted the prior banking day for more proactive management of activity

TIP: Ideal for when viewing and returning received ACH activity are necessary and when reviewing and returning the banking day after posting are not a concern

How it works:

- Received debits/credits that post to the account the prior banking day are reviewed based on profile filters
- Return decisions generate an ACH return. Pay decisions will have no impact since they are posted the prior day

AFP 2021
IN-PERSON | VIRTUAL

Additional ACH Fraud Tools - Account Validation Services

Get the confirmation needed on account status, existence and ownership

Financial Institution Contributed Data

Early Warning®

Early Warning's *National Shared Database*℠ Resource

Validates account with database

Real-time *Payment Chek*® Service

Confirm account status (checking/savings)—open, valid and active. Determine risk of return for ACH and check transactions

Real-time *Payment Chek*® Service with Account Owner Authentication (AOA)

Verify ability to transact on account—consumer or business entity

Tokenization

What is a Token

- Replaces customer payment account data with a value or “token” that can’t be traced back to an account or card within your network
- “Token” functions with internal systems as an actual card would

How it Works

- Transaction sent for approval
- Token is sent back in place of actual card number for internal processes
- Should your network be compromised, the token is of no value to hacker because they don’t have access to token issuers vault

Benefits

- Help protect customer payment data both within and outside your network
- Reduce the risk of card data exposure in the event of a data breach
- Can minimize the impact of PCI DSS Validation
- Maintain business processes that rely on cardholder data

AFP 2021
IN-PERSON | VIRTUAL

Card Fraud Mitigation

Collect → Store → Transact

Collect

Card information is captured at point of sale and online.

Encryption ●●
Protect primary account number (PAN) data in transit through your network and while it travels to Merchant Services from moment of capture at retail point-of-sale or from your website.

EMV ●
Help prevent skimming, counterfeit and lost/stolen fraud with advanced chip card technology.

Store

Card data is stored for future use.

Tokenization ●●
Protect data while at rest by replacing payment data with a secure token that cannot be converted back to card or account information within your network.

Transact

Customer identity is authenticated and fraud risks managed.

Fraud tools ●
Provide greater visibility into sophisticated fraud patterns, which can help reduce fraud and manual review and pinpoint a transaction's origin in real time and dynamic order linking.

EMV ●
EMV utilizes dynamic data that help protect transactions.

● Card-present

A type of transaction in which the card is physically swiped, tapped or dipped through a reader to capture details in person at point of sale.

● Card-not-present

A type of card transaction in which the card is not present at the point of sale for the magnetic stripe to be read.

AFP 2021
IN-PERSON | VIRTUAL

Agenda

1 Fraud Overview & Current Trends

2 Fraud Mitigation Tools

3 Tool Use Cases

4 Best Practices & Governance

AVS Use Cases

Be confident with real-time support for typical use cases

ACH Enrollment

Payroll Direct Deposit:

- Pay a new employee using account information provided for purpose of enrollment
- Validate existence of account and its status, as well as authentication of account ownership

Tax Payments

Tax payment refunds:

- Quickly validate a deposit account's existence and assess risk associated with processing the refund
- Confirm the taxpayer is the authorized owner or signor on the account

Employee Changing Bank Details

Update of account information:

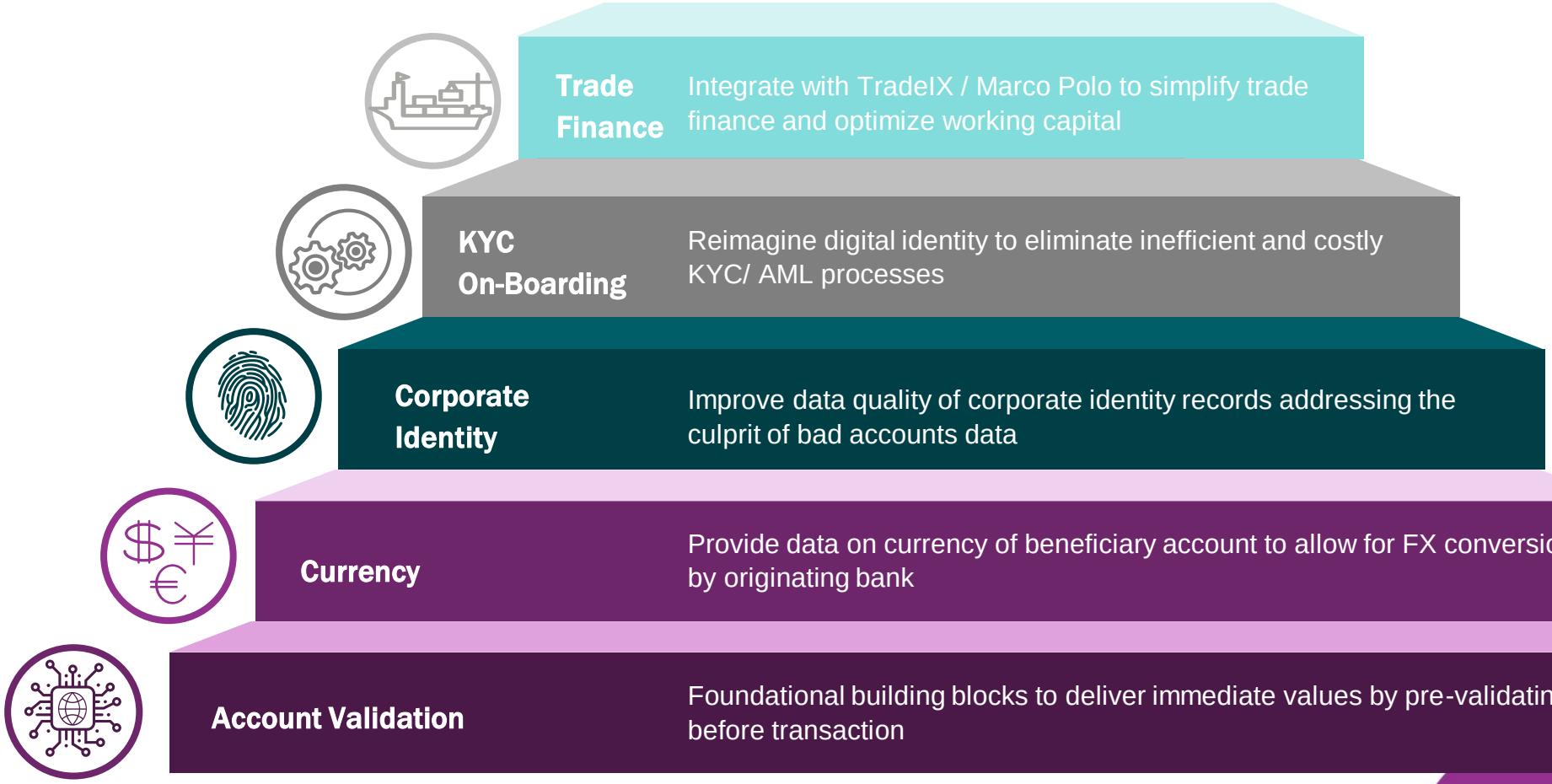
- Pay an employee using new account information provided upon change of banks
- Validate existence of account and its status, as well as authentication of account ownership

Recurring Payments

Utility payments:

- Customer provides account information for payment of monthly cable
- Validate existence of account, status, account ownership and associated risk

Potential Future Value-Added Services



Agenda

1 Fraud Overview & Current Trends

2 Fraud Mitigation Tools

3 Tool Use Cases

4 Best Practices & Governance

Fraud Prevention Best Practices

Tips to better protect your firm

1 **Conduct an independent assessment**	Engage an experienced engineering firm that understands the technical risks and complexities of enterprise architecture to do a complete technical independent assessment of your firm's infrastructure. Make sure to engage a company that has more technical expertise than a general consulting firm. You should know where your vulnerabilities are at all times
2 **Engage government and law enforcement**	Ensure you have a clear engagement model with the government including law enforcement. Who are you going to call? Which agency and under what circumstances? Have the relationship established up front and the engagement documented in a run book
3 **Join an industry forum**	Join an applicable industry-based information sharing forum ("ISAC") to share and receive important threat information
4 **Simulate an internal attack**	Create a Red Team and have them attack your systems using the same techniques the bad guys do. Not once a year, all the time. Also consider establishing a program to harvest credentials and account numbers that might be in the underground related to your bank—to detect compromises you may not otherwise be aware of
5 **Deploy mandatory employee training and testing**	Malicious email is the #1 way bad guys get into organizations. Establish a baseline training program for all employees that is mandatory and focuses on the specific actions employees need to take to protect the firm. Once you have trained your employees, actively test them.
6 **Know your third party vendors**	Understand your third party environment and upgrade your contract provisions and ensure they are following the same standards you are striving for in your own environments
7 **Exercises and drills**	Run simulations and drills to assess your capability. Use a combination of table top scenario exercises and live inject of events into your Security Operations Centres to see how it responds. Learn lessons and repeat. Include colleagues from the business in addition to technologists in the table top exercises
8 **Know how money leaves the organization**	Look at all of the ways money leaves your institution. Figure out what controls and thresholds you can put in to protect money movement assuming bad guys get around your other controls. Examples: wire limits, country destinations, new beneficiaries
9 **Implement controls for maximum effect**	Consider using resources such as Positive Pay, Reverse Positive Pay, ACH Debit Blocking, and ACH Transaction Review to provide early warning of potential fraudulent activity, allowing for faster intervention and increased likelihood of stopping transactions and recovering funds
10 **Protect your computers**	Consider physical or logical network segmentation for funds transfer related computers; employ the concept of 'least privilege" to limit the use of administrator privileges; and consider limiting the processes and services that can be run on funds transfer related computers (e.g. no email or Internet browser applications).

Best practice considerations – Payment security and controls

User access

- Make sure you know who has access to your banking relationships and accounts; review entitlements regularly
- Set payment limits at account and employee level based on payment trends/history (e.g. 12 month history)
- Establish multiple approval levels based on various thresholds (e.g. dollar amounts, tenure)
- Ensure robust and multi-level approvals required in areas such as accounts payable
- Don't have multiple users log in from the same computer to initiate or release payments
- Use approved templates/verified bank lines and restrict use of free form payments

Verification

- Don't move money based solely on an email or telephone instruction(s), even from trusted vendors
  - Validate by calling the entity requesting payment/change in instructions at their known telephone number.
    - Never call a number provided via an email or pop-up message
  - Always validate the sender's email address and hover over the email address and/or hit reply and carefully examine the characters in the email address to ensure they match the exact spelling of the company domain and the spelling of the individual's name
- Never give any information to an unexpected or unknown caller

Reconciliation

- Perform daily reconciliation of all payment activity – Immediate identification and escalation is critical

Consider establishing a program to detect anomalous payments

- Identify irregularities (e.g. first time beneficiaries, cross-border payments)
- Verify payment values and velocity
- Establish criteria to verify or release payments
- Track and trace where a payment is in the environment point to point and if altered at any time

Best practice considerations – Insurance

Two types of insurance policies to consider

- Crime - is to recover the lost money or securities. Could result from BEC and/or Social Engineering. Crime insurance is historically meant to cover malicious intent of employees for theft and fraud. Social Engineering originally not contemplated. Therefore, it is important to check if your crime insurance policy has coverage for Social Engineering and what sub limits of coverage you have. There are other riders to add to Crime Insurance such as computer crime funds transfer fraud and coverage for investigative costs.
- Cyber Liability policy should respond to a ransomware event. The policy form Cyber Extortion section can cover the ransom paid, business interruption including net income and/or extra expense), data restoration costs to repair, and property damage replacement.

NACHA Rule Updates

Supplementing Fraud Detection Standards for WEB Debits

Existing Requirement

- Originators of WEB debit entries must use a “commercially reasonable fraudulent transaction detection system” to screen WEB debits for fraud

Supplemental Requirement

- Makes explicit that a fraudulent detection system must, at a minimum, validate the account number of the account to be debited
- Will apply to the first use of an account number, or changes to the account number
- NACHA does not specify the technologies that Intuit can use to comply with the rule
  - ACH pre-notification
  - Challenge deposits
  - ACH micro-transaction verification
  - Account Validation Services
  - Artificial Intelligence and APIs

Changes to Original Proposal

- The part of the proposal to reasonably relate to the dollar amount of the purpose of payment was removed
- The effective date is **March 19th, 2022**
  - Provides 3.5 additional months from original proposal and a total of 14 months to implement
  - Applies on a “going-forward” basis to first use of new account numbers obtained for initiated WEB debits
  - Will not retroactively apply to account numbers already used for WEB debits

Key Take-Aways

1. Acceleration of fraud mitigation tools
2. Use of machine-learning to provide better outcomes
3. Instant reaction time for changing market conditions is imperative
4. Use of fraud tools on all accounts