



Nashville AFP Chapter

Best Practices for Building a Strong Security Culture and Framework

March 2020

Current threat landscape



57% of business leaders feel their organization is **more susceptible** to cybersecurity threats than previous year

Business Email Compromise (BEC)

90% of businesses were targeted and received emails related to Business Email Compromise (BEC)

136% increase in reported fraud losses related to Business Email Compromise

Ransomware

22% of corporate ransomware victims had to fully cease business operations during event

Every 40 seconds a company is hit by ransomware

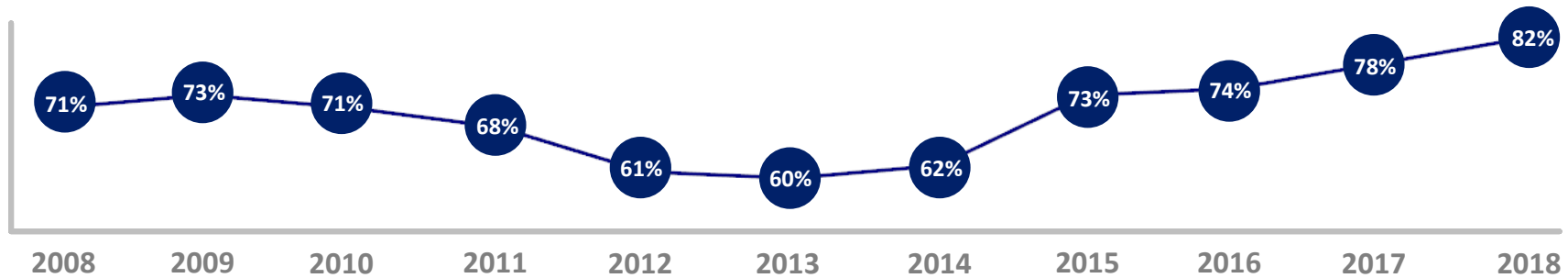
Average organization cost of **\$12M** from cyber fraud
and **\$2.4M** from malware attack

Current threat landscape

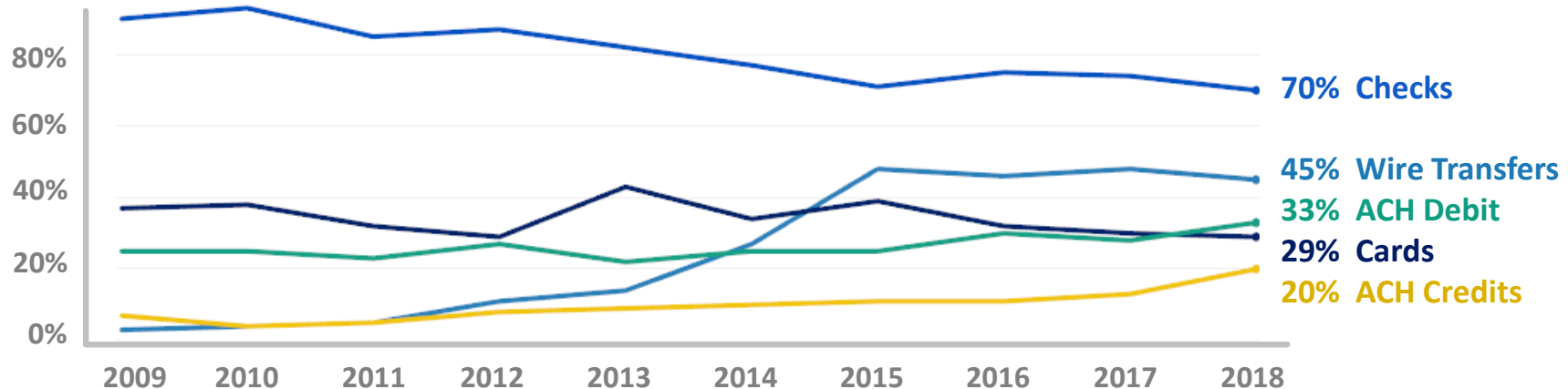
2019 AFP survey overview



A record-setting 82% of financial professionals report that their organizations experienced attempted and/or actual payments fraud in 2018.



The decline in check fraud activity has been offset by an increase in payments fraud via wire transfers and ACH debits and credits



Current threat landscape

Actors and objectives



Bad Actors and Potential Objectives



Insider

Malicious or benign, an authorized user with access to organization's data or information assets



Criminal

An individual or group who uses cyber to commit theft, fraud or other criminal acts



Hacktivist

A person or group who uses cyber activities to achieve political, social, or personal goals



Nation-state

Government-backed actors with training, resources and offensive capabilities



Fraud Schemes and Scams



The threat environment is evolving

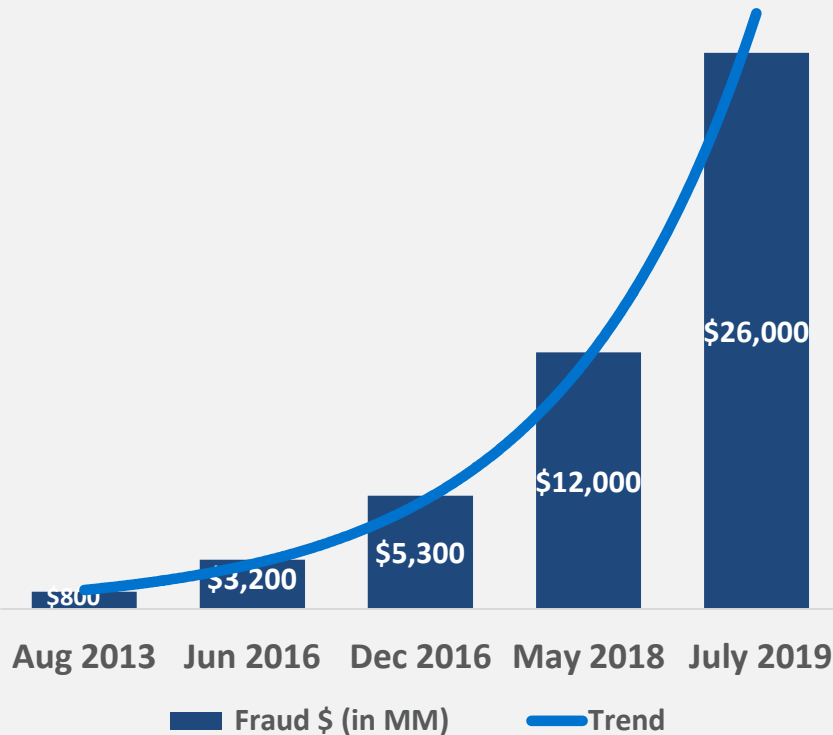
Business Email Compromise (BEC)



As of July 2019

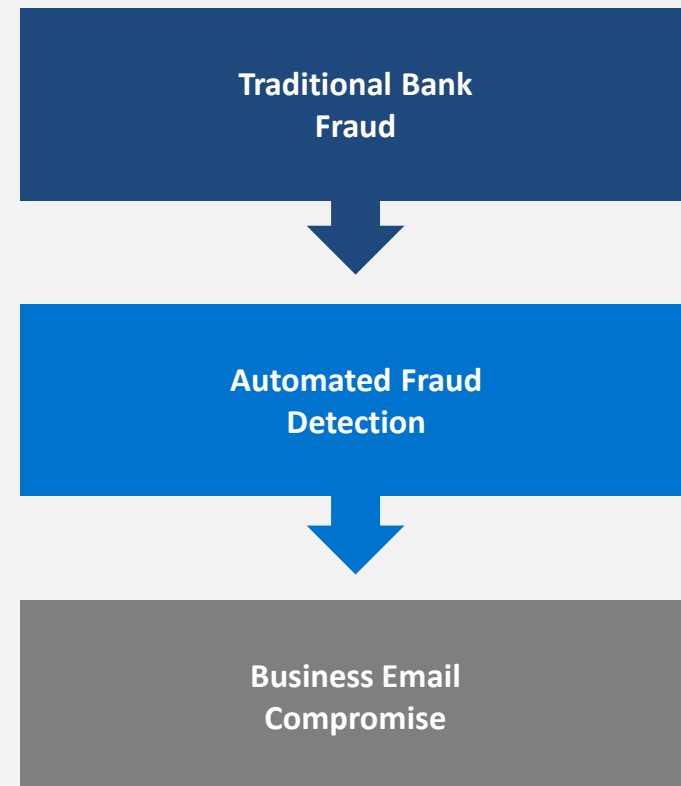
\$26.0+ Billion

Paid by BEC victims since June 2016



<https://www.ic3.gov/media/2018/180712.aspx>

Bad Actors continually find new ways to exploit defenses



Email fraud

Why it's successful



Messages Appear Highly Credible To User

- Well researched using social media
- Messages exploit the natural human tendency to trust and be helpful
- Emails use the right names & correct titles
- User similar domain names
- Custom-written to avoid spam filters



Organizations May Lack Essential Security Safeguards To Protect

- Controls such as endpoint security
- Data Encryption
- Email gateway technology to identify suspicious email



Targeted Company Lacks Essential Authentication And Controls

- Such as signature or sign-off on key controls
- Recipient ignores key procedures for fear of raising the ire of the CEO or CFO
- Employees are duped into thinking that checking on transaction might slow things down and derail a key deal



Appear From Senior Executive And Request Immediate Action

- Almost always under threshold required for a second signature
- Sometimes sent when key executive is on vacation- making an external or unknown domain name seem legitimate
- Sent when there is a company transition in the news, taking advantage of state of change

Business email compromise

Vendor “spoof” use case



Sequence of Events

1. Company receives email messages from the “sales person” of their vendor
2. Message indicates the vendor is updating their accounts receivable system and changing bank account information
3. Company replies to email as well as calls the phone number listed in the email provided for the sales person
4. Phone number did not belong to the sales person
5. Email address did not belong to the sales person

Impacts

1. Company changed account information in AP system without appropriate verification
2. Six figure payment sent to fraudulent beneficiary account
3. Vendor notified company of non receipt of outstanding bill
4. Company realized emails and phone call were with imposter posing as the vendor

HealthCare Specialty Company \$50MM Annual Revenue

From: Chris Treasurer [mailto:chris_treasurer@lrxl.cc]
Sent: Monday, March 21, 2016 10:30a.m.
To: Joe@mycompany.com
Subject: Updated Banking Information

Attention: Accounts Payable – Updated Banking Information

Joe,

We have recently completed an update to our Accounts Receivable processing. As such, please remit all payables to our updated account beginning today.

Bank: ABC123Bank

Account Number: 123456789012
Routing Number: 987654321

Email all payment confirmations to
chris_treasurer@lrxl.cc

Can you email me when this change is complete?

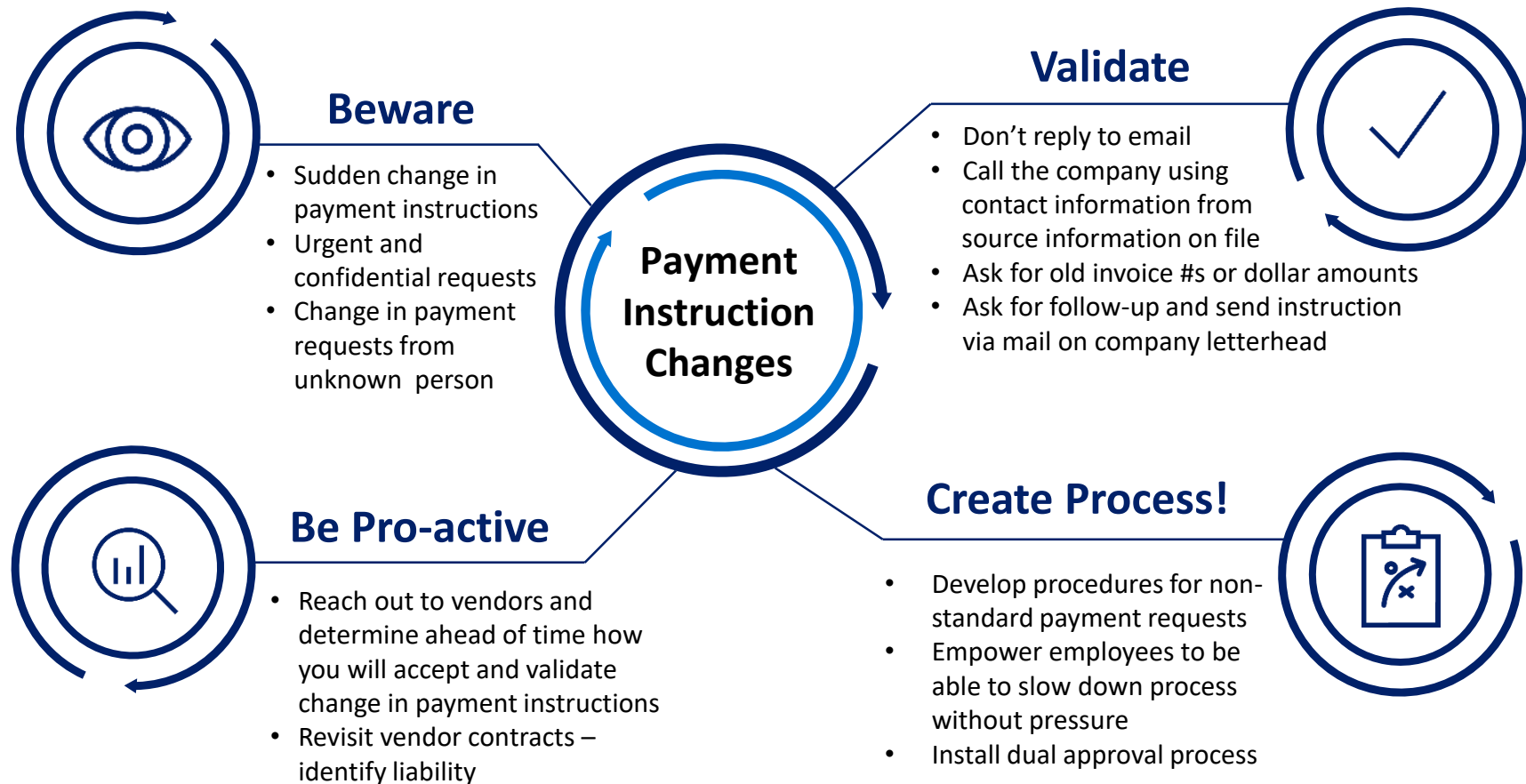
Thank You
Chris Treasurer,
Treasurer, Other Company
212.555.1212

Security Best Practices





Never reply to an email requesting a change in payment instructions





Regularly review user access



Promptly view ACH, wire and transaction notifications



Implement dual approval



Setup email alerts for ACH, wire, and balance thresholds



Establish company & user entitlement limits



Follow routines for new beneficiary instructions received via email



Review full transaction details before release



Never allow users to share computers



Tighter vendor master files on ERP



Conduct daily account reconciliation



For the highest level of security, conduct all online banking activities from a standalone, hardened and completely locked down computer



A robust vendor management program is critical to preventing data breaches.

63%

of data breaches were linked directly or indirectly to third party access.

Third parties, including contractors, suppliers, and other service providers, often act as an initial foothold for attackers, who then use that access to attack their intended target.

Source: <https://blog.securityscorecard.com/2016/07/20/third-party-vendor-breaches-2016/>

74%

of organizations have faced at least one third-party related incident in the last three years.

Source: <https://www2.deloitte.com/us/en/pages/risk/articles/extended-enterprise-risk-management-global-survey.html>

Vendor management

Best practices



What you should know about your vendor

- Who is responsible if information is breached due to vendor action or inaction?
- Who is financially liable?
- Can you shift vendors/resources and recover quickly?

Best Practices

- Perform site review; leverage security and process experts in your company
- Allow vendor access only to required data
- Limit and segregate log-ins to mitigate potential breaches
- Address responsibilities and liability if your vendor becomes compromised and impacts your business
- Understand vendor's loss recovery processes and service level agreements currently in place
- Do your homework – check references, awards, company standards regarding product, data security processes, procedures to ensure balanced risk-reward decision
- Hold your vendor to the same "Best Practice" standards you adopt internally

Protecting Your Company

Human
Resources

Operations

Information
Security

Finance

Technology




Mistakes

- Not assessing risk of breach
- No incidence response plan
- Not identifying crown jewels
- Not engaging law enforcement
- Not enough logs for analysis



Training can reduce the risk of a breach by 70%

“It’s not a matter of how much you’re being attacked, but how resilient you are.”



- Tech solution is a silver bullet
- Regulation compliance equals security
- Security is an IT issue

Common prevention myths



Use Strong Passwords

- Use at least 3 random words or 1st letter of expression or poem
- Lower and uppercase letters, numbers and symbols
- Minimum of 8 characters
- Use different passwords for different online and system accounts

Never Use Publically Available Info

- Pet's name
- Other family members' name
- Favorite holiday
- Spouse's name
- Child's name
- Place of birth
- Something related to your favorite sports team

Top Ten Passwords Most Commonly Used

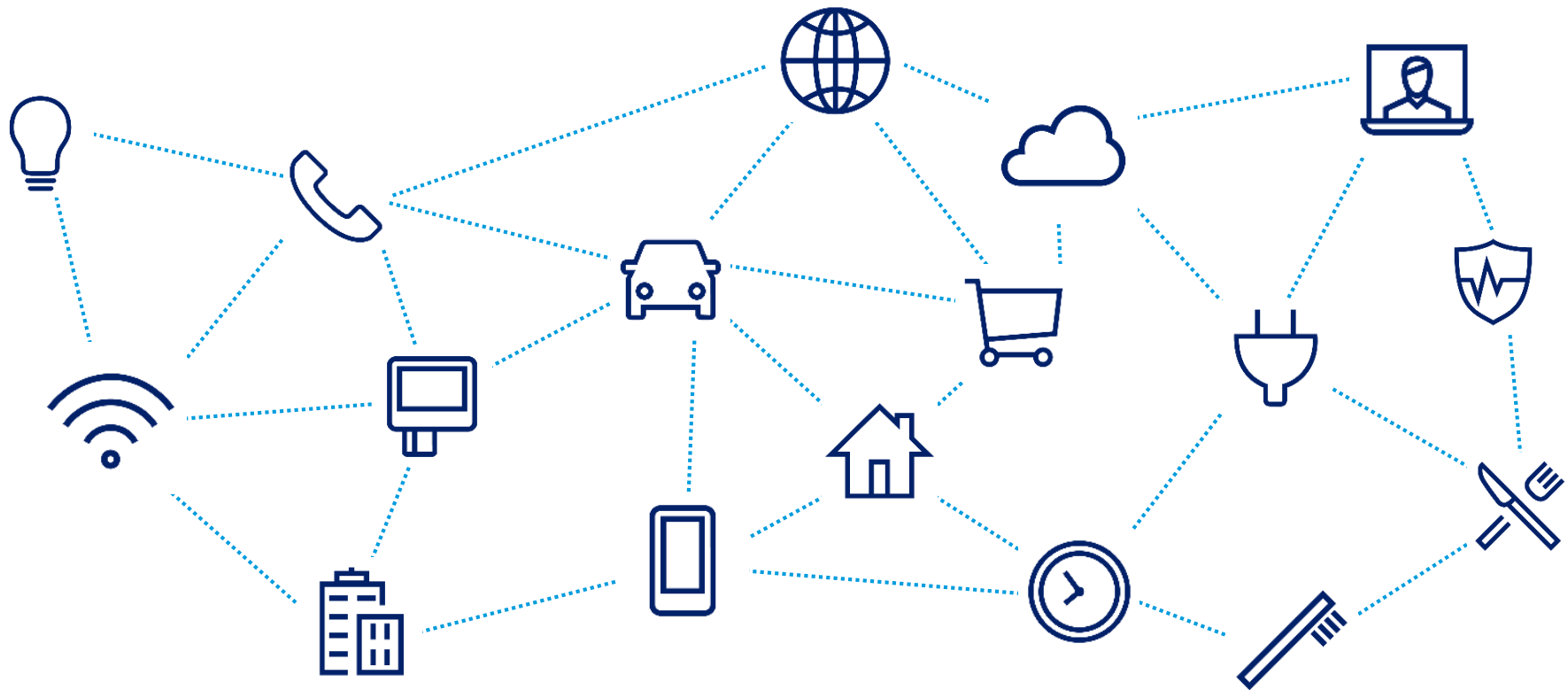
1. 123456
2. Password
3. Welcome
4. Ninja
5. Abc123
6. 123456789
7. 1345678
8. Sunshine
9. Princess
10. Qwerty

Educate your team on best practices

Internet of things (IOT)



As devices, systems and appliances increasingly communicate,
verifying trust becomes a fundamental problem



Mobile & wireless

Best practices



Attacks against mobile devices and wireless networks continue to rise as employees and consumers use mobile devices and connect to public Wi-Fi

Enable device access security	Keep OS & apps updated	Use official app stores
Enable a passcode, fingerprint or other authentication feature on all mobile devices	Recent mobile threats targeted devices with unpatched mobile OS & apps. Apply updates as soon as they are available	Apps available via untrusted app stores have a higher risk of malware. Only download from official mobile device vendor and corporate app stores
Connect through a wireless carrier	Verify Wi-Fi name before connecting	Connect through corporate VPN
Global wireless carrier networks are more secure than public Wi-Fi. Connect through your carrier when available.	When public Wi-Fi is only option, verify name of site Wi-Fi network with staff or posted signage before connecting	When connecting a business device, always use your corporate VPN or other security tools to protect your data

Turn off Wi-Fi & Bluetooth if not in use and disable image geo-tagging, rogue apps may track you



Appendix



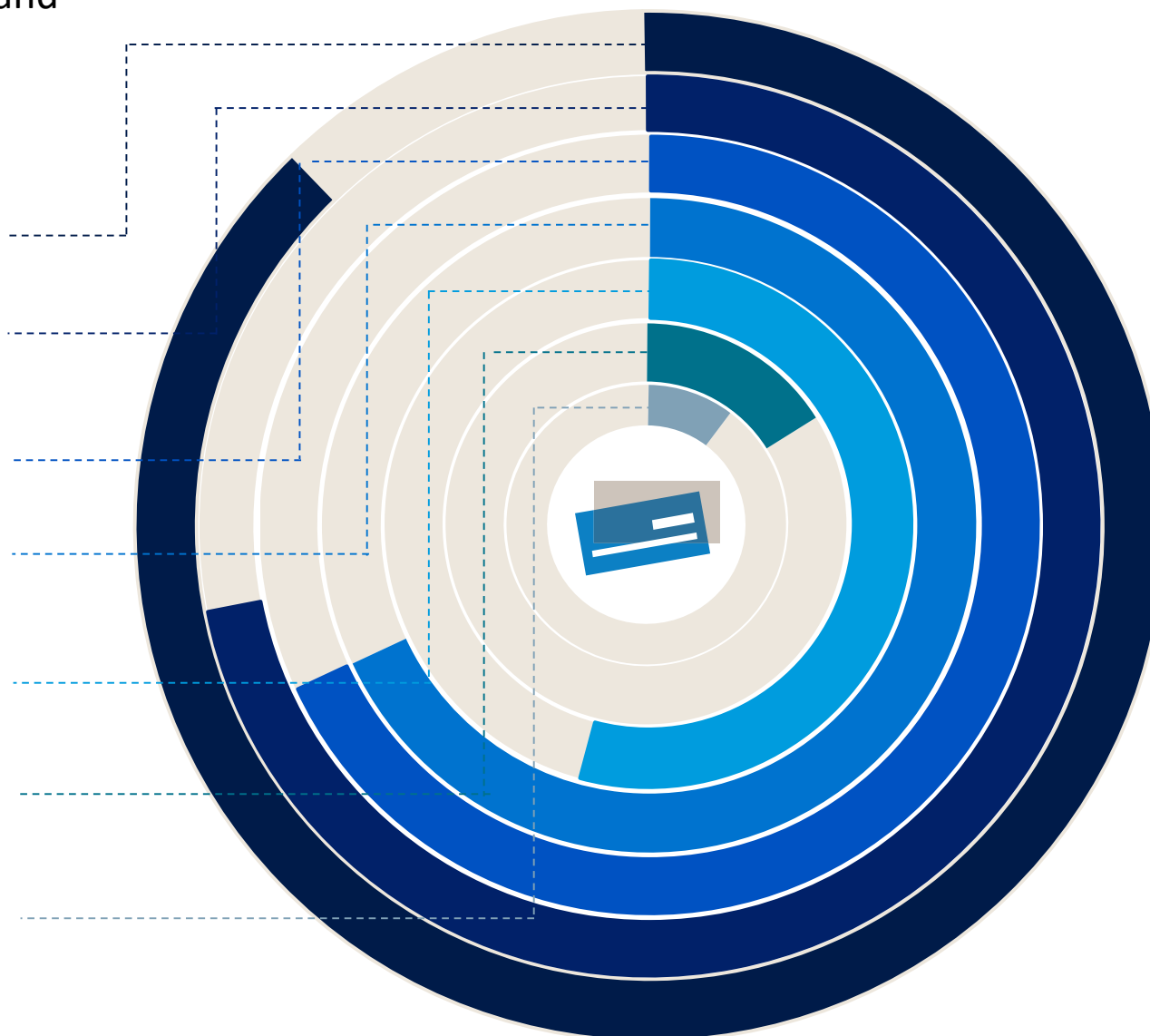
2019 AFP survey results

Check fraud control procedure responses



Fraud Control Procedures and Services Used to Protect Against Check Fraud

1. Positive Pay (88%)
2. Segregation of Accounts (72%)
3. Payee positive pay (68%)
4. Daily reconciliation and other internal processes (68%)
5. "Post no checks" restriction on depository accounts (54%)
6. Reverse positive pay (16%)
7. Non-bank fraud control services (10%)



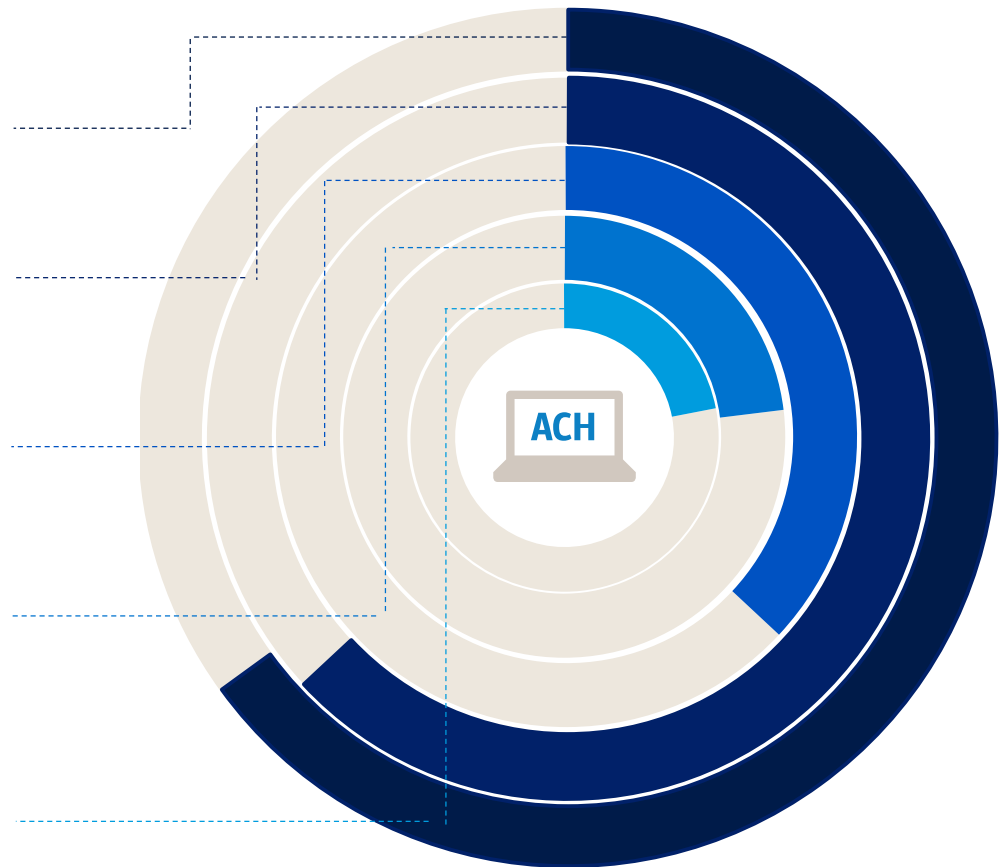
2019 AFP survey results

ACH control procedure responses



Fraud Control Procedures or Services Used to Prevent ACH Fraud

1. Reconcile accounts daily to identify and return authorized ACH debits (65%)
2. Block all ACH debits except on a single account set up with ACH debit filter/ACH positive pay (63%)
3. Block ACH debits on all accounts (37%)
4. Create separate account for electronic debits initiated by the third party (23%)
5. Debit block on all consumer items with debit filter on commercial ACH debits (22%)



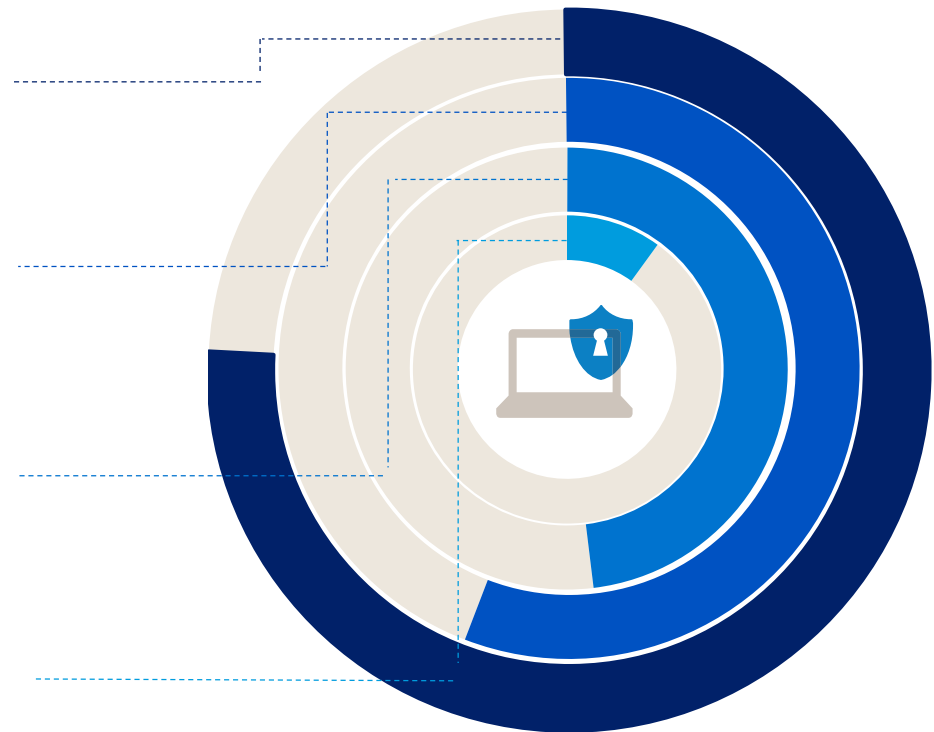
2019 AFP survey results

Security credentials defense responses



Measures Taken by Organizations to Defend Against Attacks on Security Credentials

1. Perform Daily Reconciliations (76%)
2. Ensure disaster recovery plans include the ability to continue with strong controls (56%)
3. Restrict company network access for payments to only company-issued devices (48%)
4. Dedicate a PC for payment origination (10%)



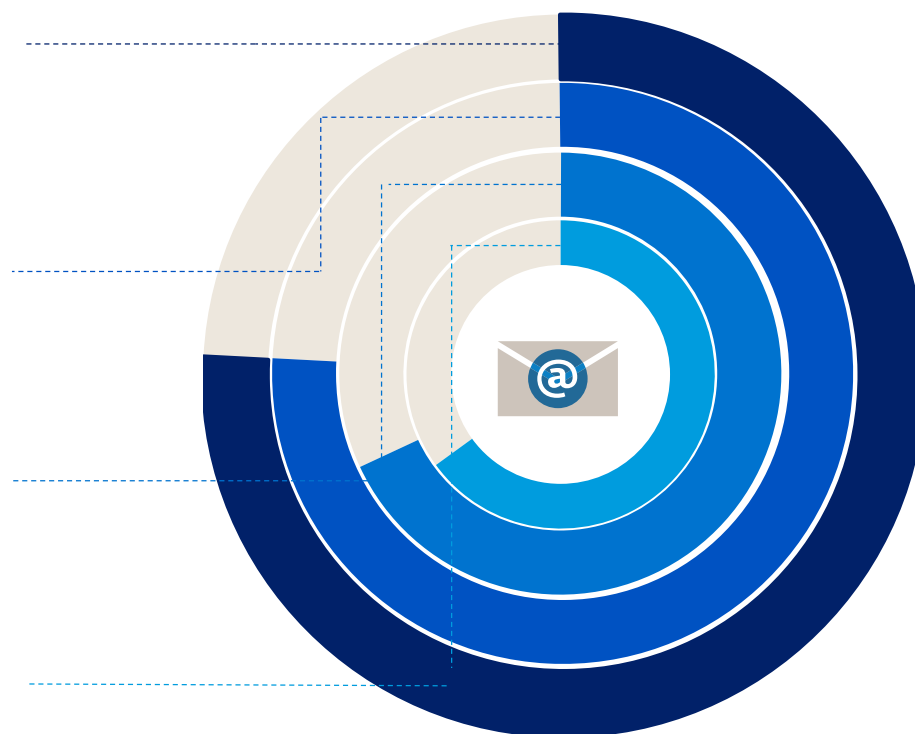
2019 AFP survey results

Email scan defense responses



Measures Taken by Organizations to Defend Against Email Scams

1. Stronger Internal Controls prohibiting payments initiation based on emails or other less secure messaging systems (76%)
2. Education and training on the BEC threat and how to identify phishing attempts (76%)
3. Implementing company policies for providing appropriate verification (68%)
4. Adopted at least a two-factor authentication or other added layers of security (65%)



Disclaimer



“Bank of America” and “BofA Securities” are the marketing names used by the Global Banking and Global Markets divisions of Bank of America Corporation. Lending, other commercial banking activities, and trading in certain financial instruments are performed globally by banking affiliates of Bank of America Corporation, including Bank of America, N.A., Member FDIC. Trading in securities and financial instruments, and strategic advisory, and other investment banking activities, are performed globally by investment banking affiliates of Bank of America Corporation (“Investment Banking Affiliates”), including, in the United States, BofA Securities, Inc. and Merrill Lynch Professional Clearing Corp., both of which are registered broker-dealers and Members of [SIPC](#), and, in other jurisdictions, by locally registered entities. BofA Securities, Inc. and Merrill Lynch Professional Clearing Corp. are registered as futures commission merchants with the CFTC and are members of the NFA.

Investment products offered by Investment Banking Affiliates:

Are Not FDIC Insured * May Lose Value * Are Not Bank Guaranteed.

This document is intended for information purposes only and does not constitute a binding commitment to enter into any type of transaction or business relationship as a consequence of any information contained herein.

These materials have been prepared by one or more subsidiaries of Bank of America Corporation solely for the client or potential client to whom such materials are directly addressed and delivered (the “Company”) in connection with an actual or potential business relationship and may not be used or relied upon for any purpose other than as specifically contemplated by a written agreement with us. We assume no obligation to update or otherwise revise these materials, which speak as of the date of this presentation (or another date, if so noted) and are subject to change without notice. Under no circumstances may a copy of this presentation be shown, copied, transmitted or otherwise given to any person other than your authorized representatives. Products and services that may be referenced in the accompanying materials may be provided through one or more affiliates of Bank of America, N.A.

We are required to obtain, verify and record certain information that identifies our clients, which information includes the name and address of the client and other information that will allow us to identify the client in accordance with the USA Patriot Act (Title III of Pub. L. 107-56, as amended (signed into law October 26, 2001)) and such other laws, rules and regulations.

We do not provide legal, compliance, tax or accounting advice.

For more information, including terms and conditions that apply to the service(s), please contact your Bank of America representative.

Investment Banking Affiliates are not banks. The securities and financial instruments sold, offered or recommended by Investment Banking Affiliates, including without limitation money market mutual funds, are not bank deposits, are not guaranteed by, and are not otherwise obligations of, any bank, thrift or other subsidiary of Bank of America Corporation (unless explicitly stated otherwise), and are not insured by the Federal Deposit Insurance Corporation (“FDIC”) or any other governmental agency (unless explicitly stated otherwise).

This document does not constitute investment advice or a recommendation or an offer or solicitation, and is not the basis for any contract to purchase or sell any security or other instrument, or for Investment Banking Affiliates or banking affiliates to enter into or arrange any type of transaction as a consequent of any information contained herein.

With respect to investments in money market mutual funds, you should carefully consider a fund’s investment objectives, risks, charges, and expenses before investing. Although money market mutual funds seek to preserve the value of your investment at \$1.00 per share, it is possible to lose money by investing in money market mutual funds. The value of investments and the income derived from them may go down as well as up and you may not get back your original investment. The level of yield may be subject to fluctuation and is not guaranteed. Changes in rates of exchange between currencies may cause the value of investments to decrease or increase.

We have adopted policies and guidelines designed to preserve the independence of our research analysts. These policies prohibit employees from offering research coverage, a favorable research rating or a specific price target or offering to change a research rating or price target as consideration for or an inducement to obtain business or other compensation.

© 2019 Bank of America Corporation. All rights reserved.