A Different Kind of Social Security – Protecting Your Business from Social Engineering Fraud

Webcast

June 2019

Bank of America
Merrill Lynch

Speakers

Tom Durkin is a Managing Director for Digital Channels Product Management at Bank of America Merrill Lynch. Durkin leads his team in developing client centric strategies and technology initiatives for all Channels offered through the CashPro platform.

Durkin also chairs Bank of America Merrill Lynch's client advisory boards for the CashPro Channels. This forum represents clients across all lines of business from FI, and Global Multinationals to Business Banking.

Aubrey B. Farrar Sr., is currently employed as Senior Vice President; Sr. Tech Mgr-Info Security Engr of the Global Technology and Operations for the Bank of America. Mr. Farrar has honorably served in the United States Air Force Reserve, United States Marine Corps (USMC), as well as, twenty-eight (28) years of previous law enforcement experiences in a wide range of criminal and national security computer intrusion investigations.
As the Assistant Section Chief of the FBI's Cyber Operations Section since 2014, he was responsible for leading the FBI's efforts to identify, pursue, and defeat cyber adversaries targeting global U.S. interests.

Mary Rosendahl is a director in the Digital Channels team in Global Transaction Services at Bank of America Merrill Lynch. Mary's responsibilities include overseeing the security authentication roadmap and overall risk management for the bank's online banking portal, CashPro®. Mary also designs the fraud prevention curriculum for the bank's corporate, commercial and financial institution clients, and is a regular speaker at industry events on the topic.

Bank of America
Merrill Lynch

Agenda

- Fraud Landscape
- Cyber Security Predictions
- AFP Fraud Study
- Security Best Practices

Bank of America
Merrill Lynch

Evolving Cyber Crime Trends

Recent History of Cyber Crime Events

Bank of America Merrill Lynch

In 1989, the first cyber attack was launched. Since then, the tactics and intent have become more sophisticated and malicious, and the stakes are higher.

2014

- Chinese hackers **exploit vulnerability** to steal 4.5M patient records
- North Korea attacks Sony Pictures
- Yahoo data breach 3B accounts
- Cyber criminals exposed **76M account details** – JP Morgan Chase

2015

- Apple customers in China fall victim to **malware infected applications**
- FDIC employee puts thousands of **confidential records at risk**
- 230K+ Ukrainians lost electricity due to a Russian cyber attack
- 78M customers' data compromised – Anthem Inc., US healthcare provider

2016

- Thieves steal 1.5M Verizon **customers' information**
- **$81M stolen from Bank of Bangladesh** due to North Korean attacks via the SWIFT network
- 19.2K emails stolen and leaked from the Democratic National Committee by Russian state-sponsored actors

2017

- **Ransomware or wiper attacks** such as WannaCry and NotPetya have plagued major government agencies, healthcare institutions and multinational companies
- 1.34B email accounts exposed inadvertently by River City Media
- $9.5M in losses due to a single Business Email Compromise (BEC) incident – MacEwan University
- Equifax's data breach exposed **143M people to identity theft**

2018

- **Cosmos Bank** cyber heist results in loss of $13.5 million. First known instance of an ATM cash out operation accompanied by a SWIFT-related attack
- **Facebook notified 87M members** that their data had been shared (though likely many more)
- Upwards of 150M MyFitnessPal users had their information compromised in the Under Armour data breach
- FBI reported $12B+ in losses due to BEC between Oct. 2013-May 2018

Data source:
https://beta.theglobeandmail.com/globe-investor/investment-ideas/cybersecurity-a-growing-risk-for-canadian-stocks/article36049361/?ref=http://www.theglobeandmail.com&
http://www.businessinsurance.com/article/00010101/NEWS06/912316064/Perspectives-Tallying-the-true-cost-of-the-Equifax-breach
https://blog.barkly.com/biggest-data-breaches-2018-so-far
https://www.ic3.gov/media/2018/180712.aspx

Evolving Cyber Threats

Bank of America Merrill Lynch

Business Email Compromise (BEC) and financial malware volumes will remain elevated, with threat actors motivated by the success of their past fraudulent activities and benefiting from the development of new techniques to avoid detection.

Cyber threats targeting mobile devices will continue to increase in both complexity and frequency as the mobile attack surface area continues to be augmented with new devices.

Greater availability and growing global instability will result in increased technical sophistication of destructive malware operations, along with increased use of destructive malware in regional conflicts.

Emerging technologies will shape the cyber threat landscape, as technologies such as Artificial Intelligence (AI) and crypto currencies have a continuing impact on the nature of cyber threats.

Breaches of third parties will continue to pose a threat to all organizations, while supply chain attacks will continue to increase in frequency over time.

Following a year of public policy proposals to develop new or expand existing laws, rules, and regulations on cyber, data, privacy, and information security, the policy and regulatory landscape will continue to change internationally throughout 2019.

Threat Landscape

Bank of America Merrill Lynch

Insider

Malicious or benign, an authorised user with access to organisations 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

Potential Objectives

Steal

- Gain assets or data
- Release data to the public
- Create a competitive advantage
- Extort money

Disrupt

- Halt critical services
- Interrupt business processes
- Embarrass the company

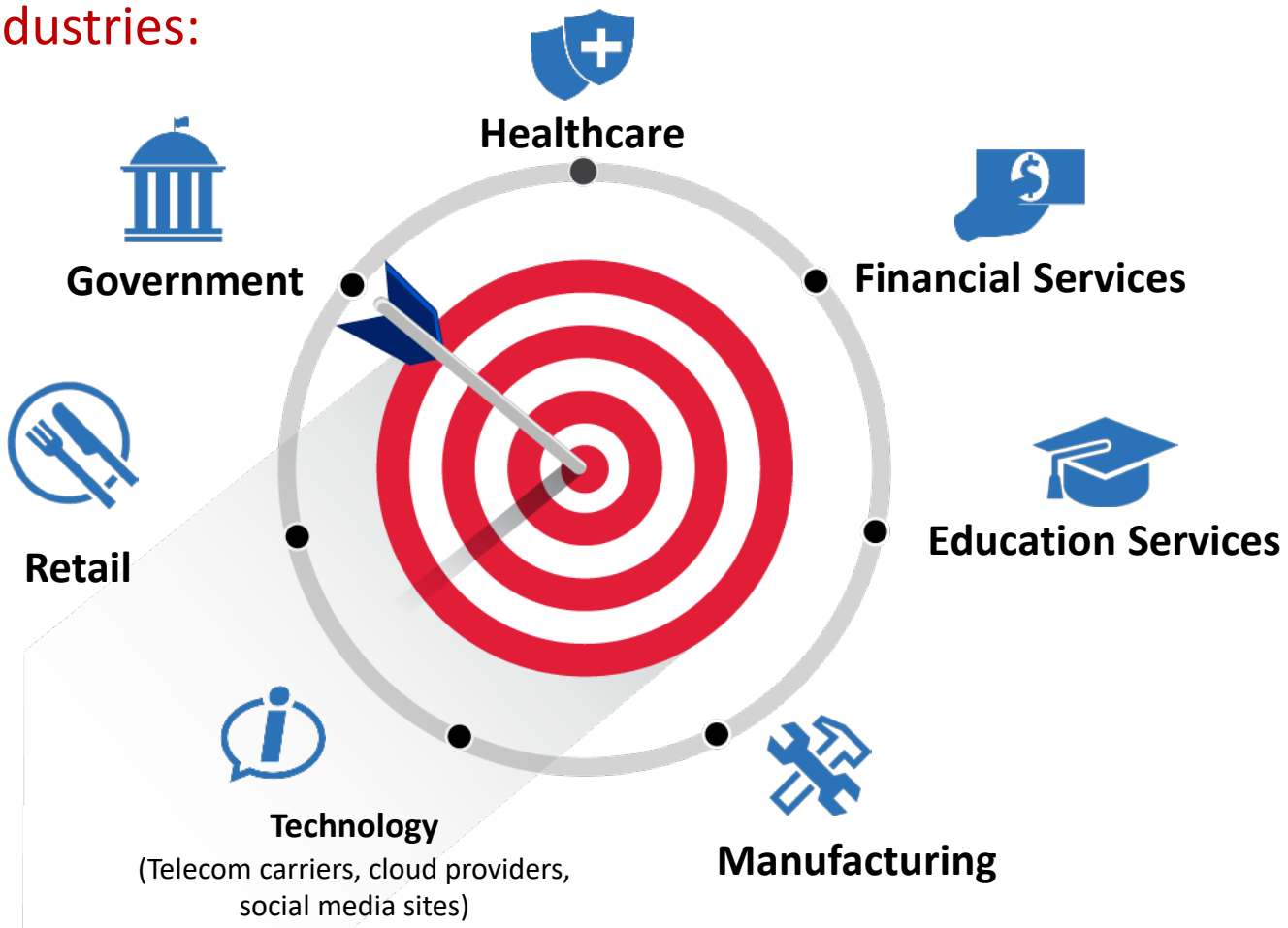
Destroy

- Destroy assets
- Create a political advantage
- Discredit and harm the company's reputation

Cyber Crime Affects Multiple Industries

Bank of America Merrill Lynch

Top targeted industries:



The Financial Services Sector represents a vital component of our nation's critical infrastructure. Large-scale power outages, recent natural disasters and an increase in the number and sophistication of cyber attacks demonstrate the wide range of potential risks facing the sector. *(Source: DHS.gov)*

Data source: 2017 Ponemon Institute Cost of Data Breach Study

Real Impact of Cyber Crime

Bank of America Merrill Lynch

Cost of Cyber Crime[1]

	2017	2018
Internet-Enabled Theft, Fraud	$1.4 Billion	$2.71 Billion
BEC/Email Account fraud losses	$676 Million	$1.2 Billion
Fraud/Romance Schemes	$211 Million	$363 Million

Cyber Attack Trends[2]

12% to 23%
Nation-State Increased between (2017) to (2018)

12X
C-Suite Executives More likely targeted by social engineering attacks than other employees

21%
Cloud Platforms Contributed to breached due to misconfigurations

13% to 25%
Cyber-Espionage Data Breach Increases

24%
Ransomware Malware Related Breaches- Second Biggest Threat

32% to 78%
Phishing Cyber Espionage Incidents

1 - 2018 FBI Internet Crime Report - https://www.fbi.gov/news/stories/ic3-releases-2018-internet-crime-report-042219

2 - 2019 Verizon Data Breach Investigations Report - https://enterprise.verizon.com/resources/reports/dbir/

Law Enforcement Response to Cyber Crime

Bank of America Merrill Lynch

THE WALL STREET JOURNAL.

U.S. Edition ▾ | May 30, 2019 | Print Edition | Video

Home World U.S. Politics Economy Business Tech Markets Opinion Life & Arts Real Estate WSJ. Magazine

U.S.

Officials Arrest Dozens in Email Scam Aimed at U.S. Businesses

Over 70 people in the U.S. and Nigeria have been arrested in scam that cost companies hundred of millions

U.S. officials said an email scam originating in Africa has targeted American businesses and cost victims hundreds of millions of dollars.
PHOTO: JIM BOURG/REUTERS

U.S. CASE EXAMPLES

May & June 2018

Southern District of Florida charged 23 individuals with laundering at least $10 million from BEC scam proceeds - including ~$1.4 million from a Seattle corporation, title companies and a law firm.

Southern District of Georgia charged two Nigerian nationals residing in the U.S. with defrauding a real estate closing attorney - sending spoofing emails posing as the seller - requesting proceeds of a real estate sale of $246,000 be wired to defendant's account – actually a fraudulent account.

https://www.wsj.com/articles/officials-arrest-dozens-in-email-scam-aimed-at-u-s-businesses-1528747102

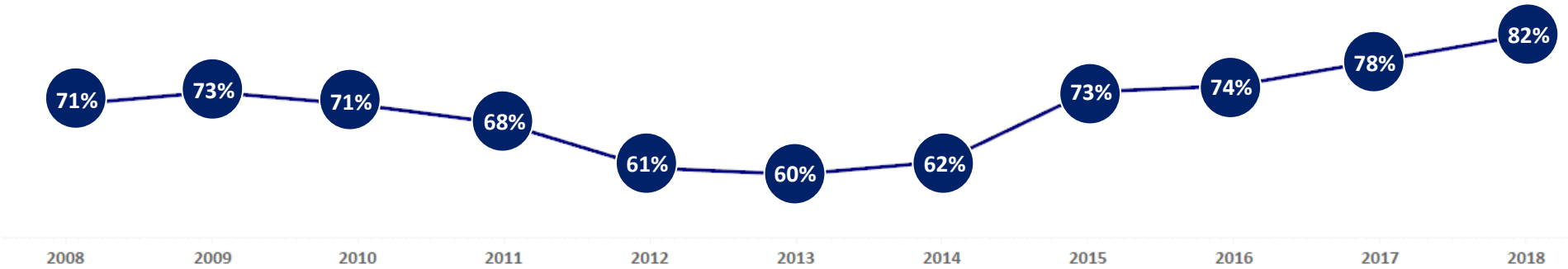
Bank of America
Merrill Lynch

2018 AFP Fraud Study

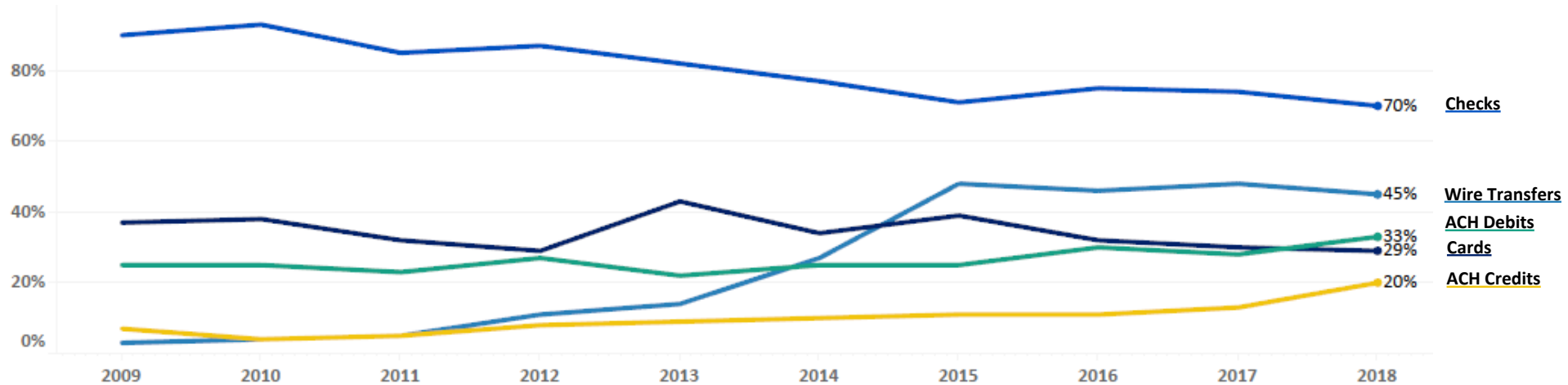
Payment Fraud in 2018

Bank of America Merrill Lynch

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*:



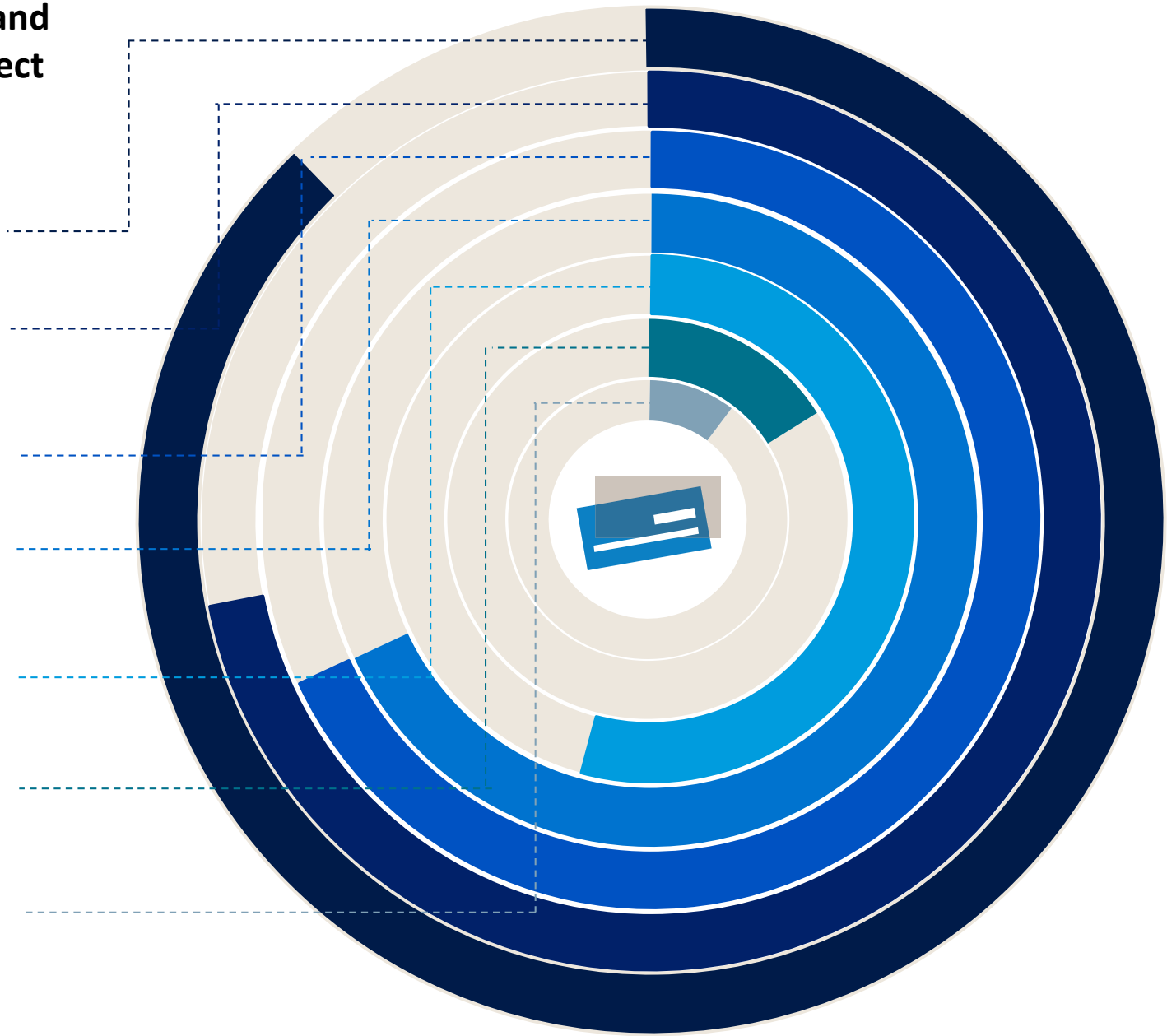
*2019 AFP® Payments Fraud and Control Survey

Check Fraud Control Procedure Responses

Bank of America Merrill Lynch

Fraud Control Procedures and Services Used to Help 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%)



ACH Fraud Control Procedure Responses

Bank of America Merrill Lynch

Fraud Control Procedures or Services Used to Help Prevent ACH Fraud

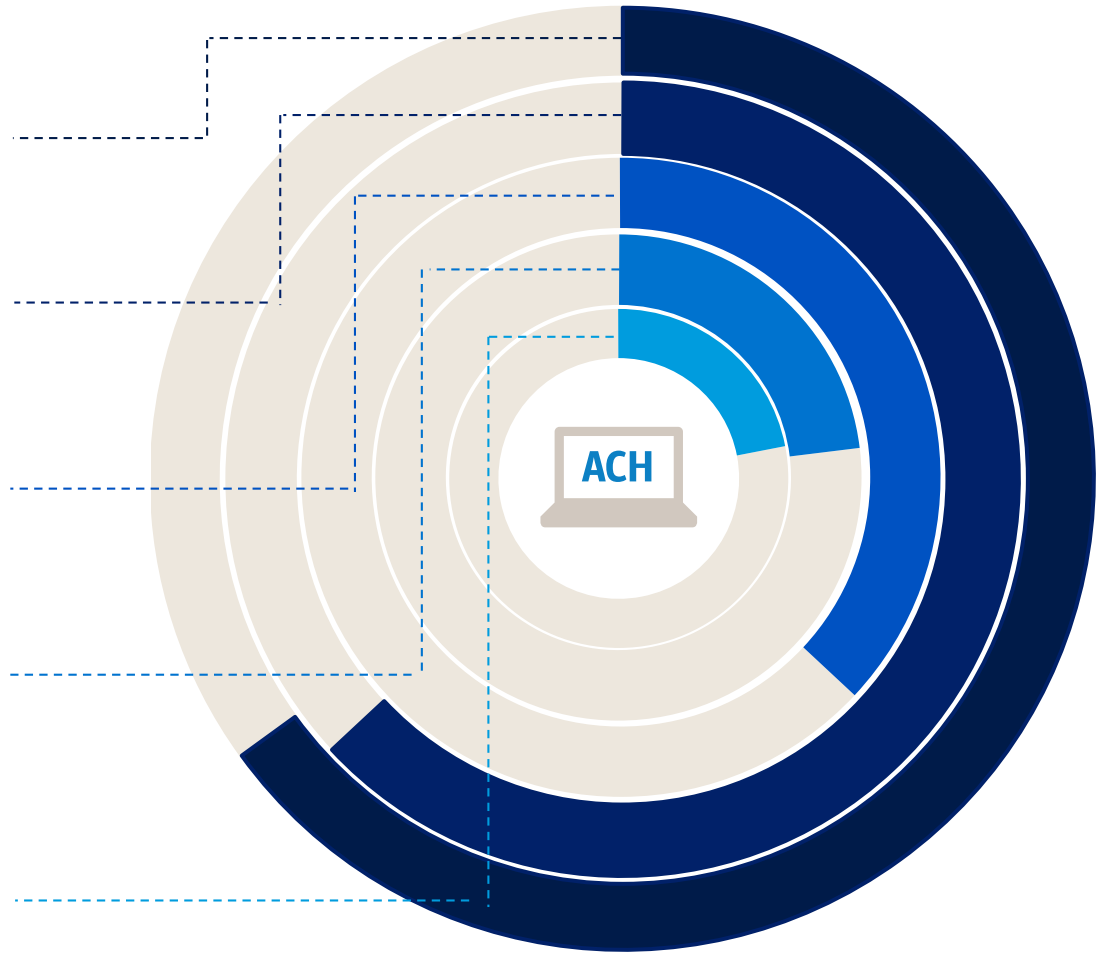
1. Reconcile accounts daily to identify and return authorized ACH debits (65%)

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%)



Security Credentials Defense Responses

Bank of America Merrill Lynch

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%)

Email Scam Defense Responses

Bank of America Merrill Lynch

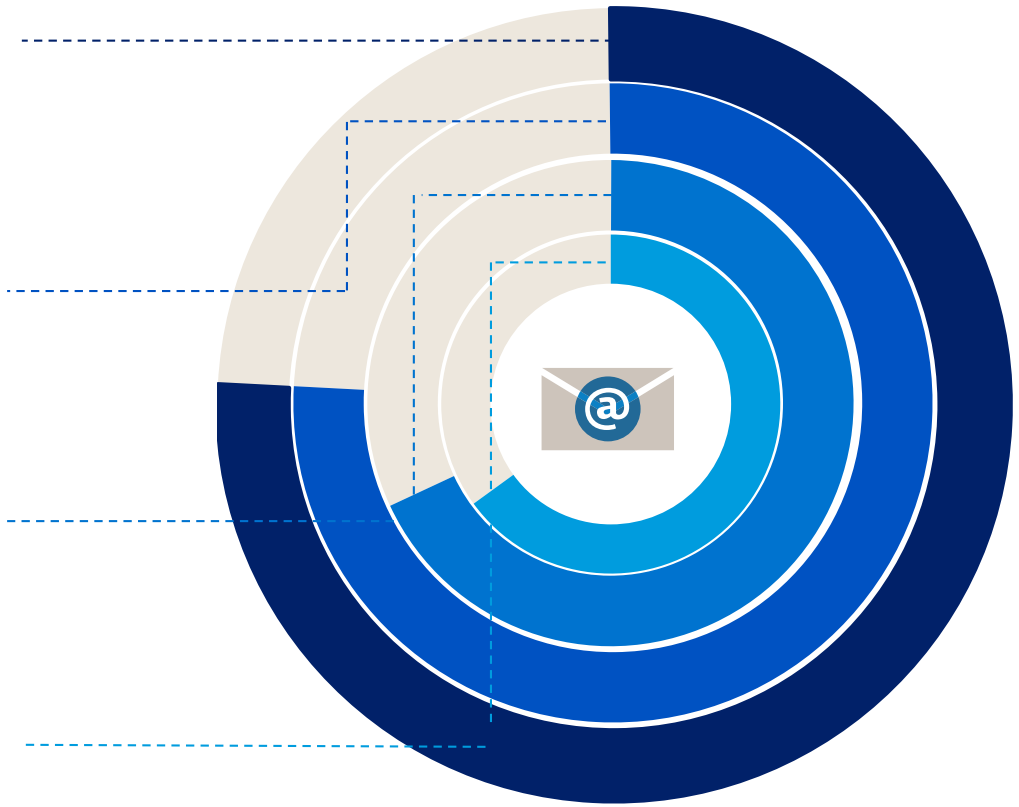
Measures Taken by Organizations to Defend Against Email Scams

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%)



Bank of America
Merrill Lynch

Security Best Practices

Fraud Landscape

Cyber attacks are the fastest growing crime

Cyber intrusions are becoming more commonplace, more dangerous, and more sophisticated. The threat is incredibly serious—and growing.

$5.2 Trillion

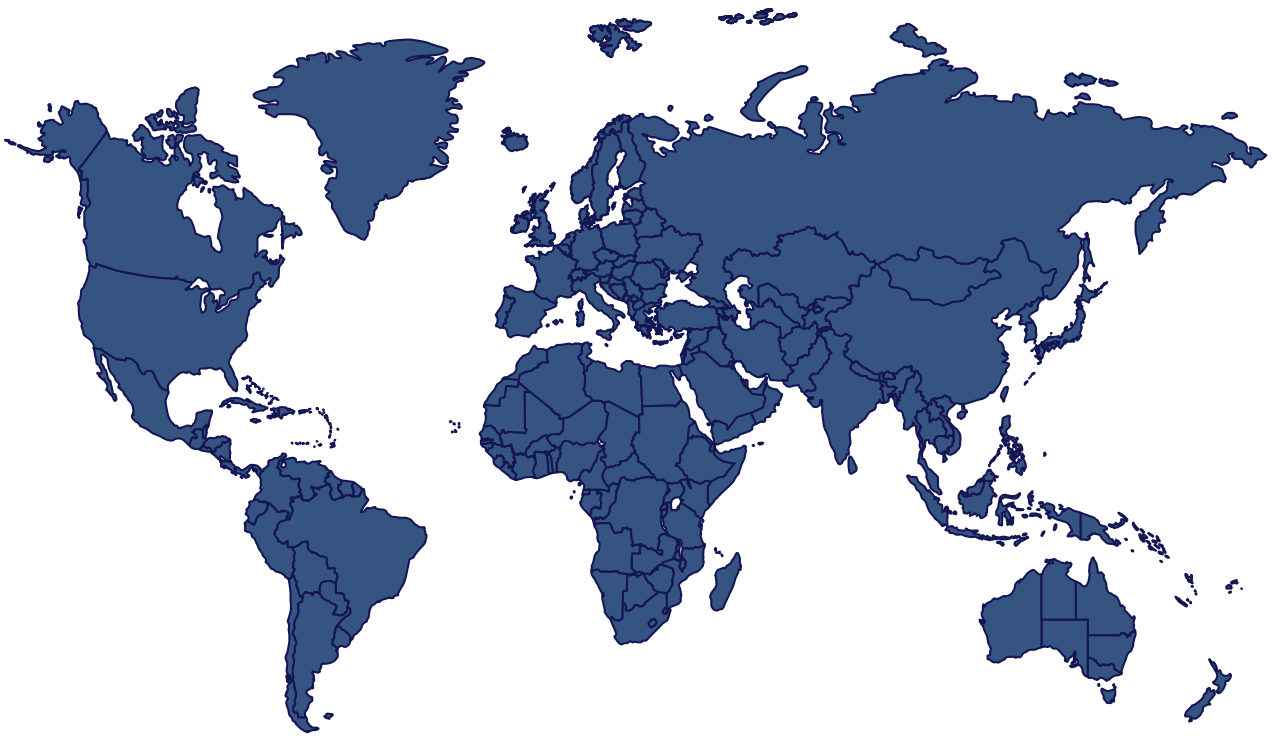
Cost to companies globally over next 5 years [1]

14 seconds

Predicted frequency of a business falling victim to a Ransomware attack in 2019 [2]

1,300%

Increase in identified exposed losses due to Business Email Compromise since 2015 [3]



[1]https://www.apnews.com/ac9bb114045c49c59089abae155045e4

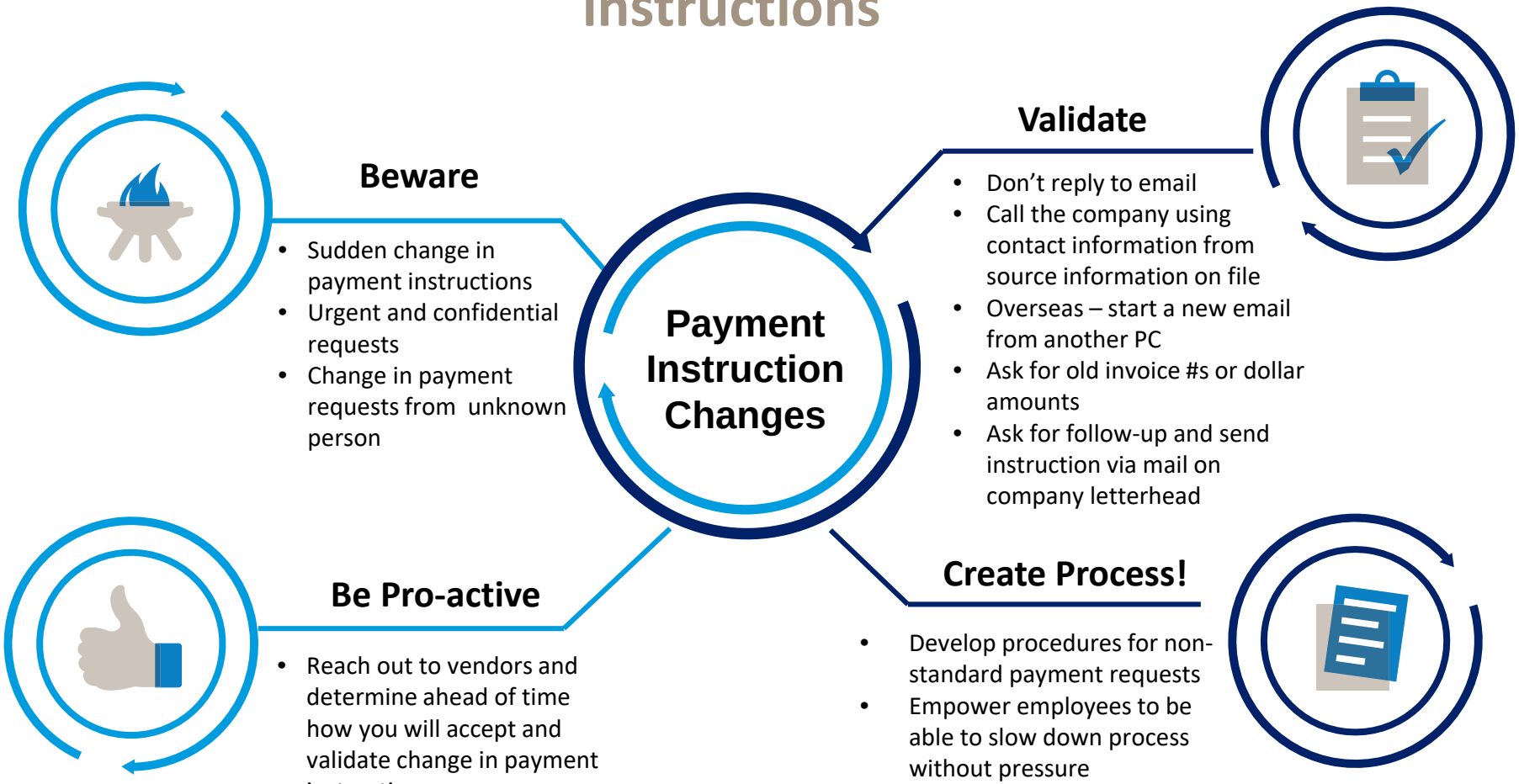
[2]https://cybersecurityventures.com/ransomware-damage-report-2017-part-2/

[3]https://www.fbi.gov/news/stories/business-e-mail-compromise-on-the-rise

Best Practices for Business Email Compromise

Bank of America Merrill Lynch

Never reply to an email requesting a change in payment instructions



Social Engineering

Bank of America
Merrill Lynch




What is Social Engineering?

Social engineering is the art of manipulating people so they give up confidential information.

Social engineering criminal attacks happen at work, home, in person, and on mobile devices.

- ✓ What do social engineers want?
- ✓ Why do they do this?

Social Engineering

Bank of America Merrill Lynch

System Thinking

- System 1
  - Very fast, instant
  - 95% of our thoughts
- System 2
  - Requires us to be engaged
  - Deliberate thoughts

As technology improves, people are the low hanging fruit.

Fraudsters use:

- Change blindness
- Filtering
- Emotional news reports
- Risk gap

Social engineering takes advantage of the human and our weakness

Social Engineering

Bank of America Merrill Lynch

89% of organizations have experienced a data breach almost 2/3 as direct result of employee error*

Ongoing education is critical to success

Integrated into company DNA

Training as often as culture will tolerate

Nudge theory training

Fraud detection becomes “system 1” thinking

Display hints at most relevant points of behavior

Reward performance, have “phish detection” competitions

Training before any employee talks on the phone or accesses the internet

Security ambassadors

Share fraud events – employees need to see it’s real

https://pressreleases.responsesource.com/news/97714/eighty-nine-percent-of-organisations-have-experienced-a-data-breach/

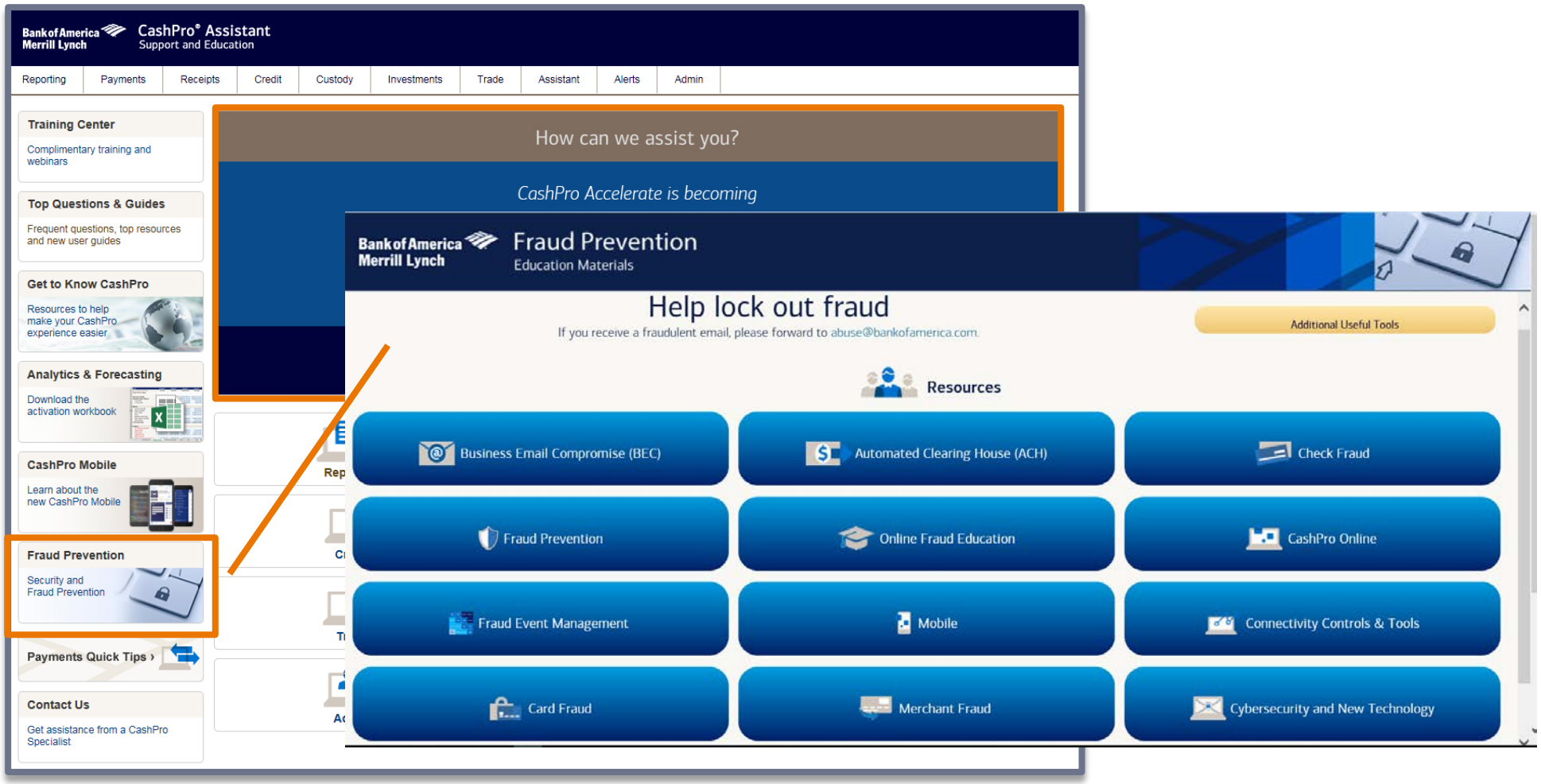
Maintaining a Cyber Defense Framework

Bank of America Merrill Lynch

	PEOPLE	PROCESSES	TECHNOLOGY
PREPARE	• HR (Cyber Team & Screen Insider Threat) • Cyber Awareness Program (Basics) • Tabletop Exercises: Cyber Scenarios • Exec/Board of Directors (BoD): Priorities	• Cyber Security Policies/Risk Management • Identify Value (Crown Jewels) • Regulatory Compliance • Cyber Insurance Considerations	• Map Assets (Network/Systems/DBs) • Implement Access Control • Isolate Web-Facing from Internal Systems • Reduce Network Points-of-Entry • Register Similar Domains (prevent spoofing)
PREVENT	• Cyber Intelligence (Cyber Intel) • Red Team: Test System Security • Least Privilege & Separation of Duties • Restrict Social Media/Risky Websites	• Risk/Cyber Threat Assessments • Governance/Audit: Program Compliance • 3rd Party (Vendor/Partner) Assessments	• Vulnerability Scanning/Patch Management • Encrypt Communications (VPN) & Data-at-Rest • Information Back-Up (Ongoing & Tested) • Remote Access: Isolate/Restrict
DETECT	• 24/7 Incident Response Team • Employee Phishing Simulation Tests • Hunt Team (Vulnerability Search)	• Cyber Incident Reporting & Notification • BEC Processes & 2-Person Checks • Fraud ID & Handling Processes	• Alerting: Cyber Intel Indicators In Place • Network & Cloud Intrusion Detection • Email Phishing/Spam Detection/Containment • Cyber Event Logging: Network & Cloud
MITIGATE	• Cyber Event: Clear Roles & Responsibilities • Leadership Escalation Communications	• Event Containment Processes	• Dynamic Access & Malware Blocking • DDoS Mitigation
RESPOND / RECOVER	• Communications to Execs/BoD • External Communications (PR) • After-Event Assessments • ID Gaps: Update Employee Training/Skills	• Escalation Procedures • Business Continuity/Disaster Recovery • Update Policies - Lessons Learned	• Restore Back-ups: Lost/Corrupted data • Post-Event Forensics Investigation

CashPro® Assistant

Fraud Prevention Resources



Not a CashPro user? Visit www.bofaml.com/fraudandcybersecurity

Bank of America
Merrill Lynch

Discussion and Q&A

Notice to Recipient

Bank of America Merrill Lynch

"Bank of America Merrill Lynch" is the marketing name for the global banking and global markets businesses of Bank of America Corporation. Lending, derivatives, and other commercial banking activities are performed globally by banking affiliates of Bank of America Corporation, including Bank of America, N.A., Member FDIC. Securities, 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., Merrill Lynch, Pierce, Fenner & Smith Incorporated, and Merrill Lynch Professional Clearing Corp., all of which are registered broker-dealers and Members of SIPC, and, in other jurisdictions, by locally registered entities. BofA Securities, Inc., Merrill Lynch, Pierce, Fenner & Smith Incorporated 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 Merrill Lynch 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 is intended for information purposes only and 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.