# Security and Fraud Prevention

Bank of America Merrill Lynch

October 2018

Bank of America
Merrill Lynch

# Agenda

- Evolving threat landscape
- Fraud schemes and scams
- Security best practices

Bank of America
Merrill Lynch

# Cyber Threat Trends

**57%** of business leaders feel their organization is **MORE SUSPECTIBLE** to cybersecurity threats in 2018 than previous year

**$12.5 Billion**
Business Email Compromise

**$2.4 Million**
Average organization cost from malware attack

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

**59%** of malicious email sent contained a banking Trojan surpassing ransomware for the first time since 2016

Companies are hit by ransomware every **40 seconds**

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

**$12M** Average organization cost from cyber fraud

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

hxxps://www[.]ic3[.]gov/media/2018/180712.aspx
hxxps://threatconnect[.]com/wp-content/uploads/ThreatConnect-Building-a-Threat-Intelligence-Program.pdf
hxxps://www[.]Malwarebytes[.]com/pdf/infographics/Malwarebytes_The_State_Of_Ransomware_Among_SMBs.pdf
hxxps://www[.]Proofpoint[.]com/sites/default/files/pfpt-us-tr-q118-quarterly-threat-report.pdf
Ponemon Institute 2018 State of Endpoint Security Risk Report

# Current Threat Landscape

## Actors

### Insider

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

### Criminal

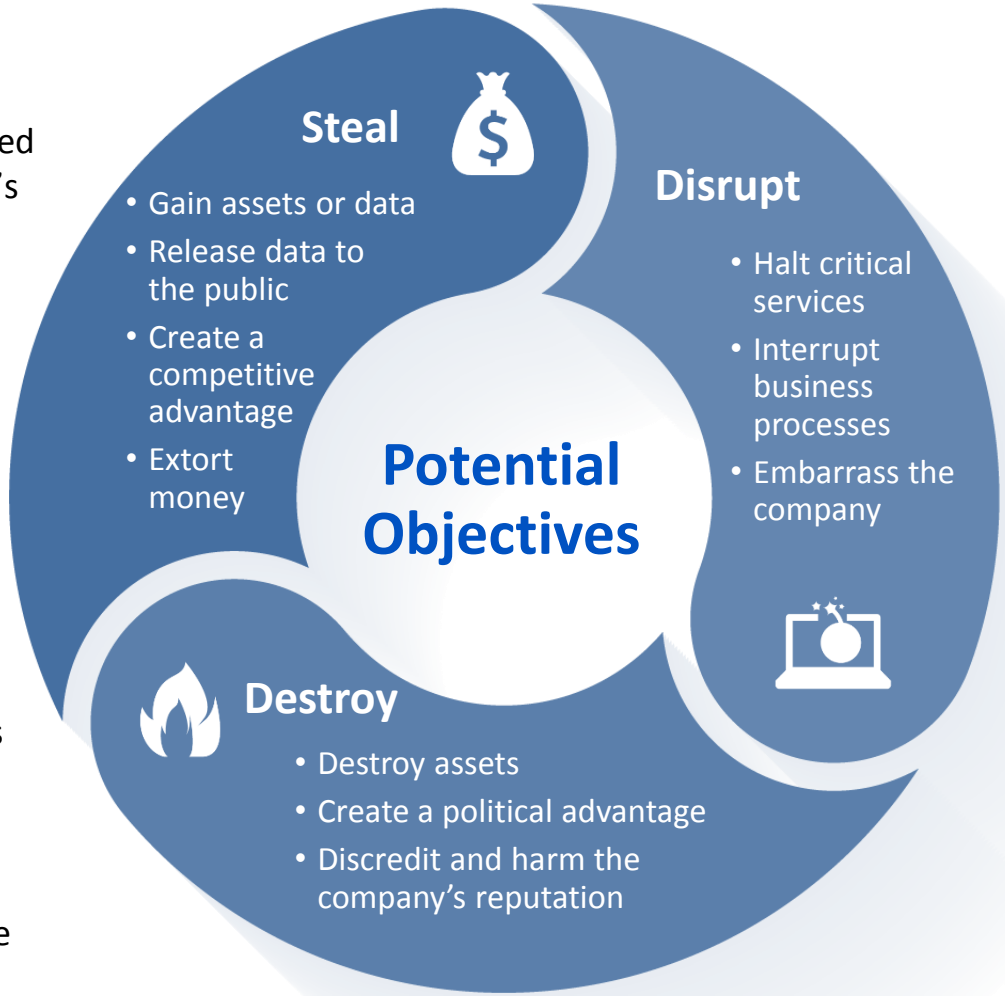
An individual or group who uses cyber to commit theft, fraud or other criminal acts

### 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



# Recent History of Cybersecurity Events

**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
- Cybercriminals 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

# Cyber Attacks

## Prevention

### Biggest mistakes companies make

- Not assessing risk of breach
- No incident response plan
- Not identifying crown jewels
- Nothing available for analysis
- Not engaging law enforcement

34K
Number of cybersecurity incidents that happen daily in the US

Training can reduce the risk of a breach by 70%

### Common prevention myths

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

**"It's not a matter of how much you're being attacked, but how resilient you are."**

The Art of Incident Response; Partner Focus ACCESS Data. May 2018

# Security Program Considerations

**Cyber and fraud events** can have major impacts on revenues, earnings and reputation. Consider these elements of a cybersecurity program.

## PREPARE — Processes to manage risk

- Identify critical assets
- Corporate Governance
- Engage Sr leadership and Board
- Risk Management strategy
- 3rd Party/Vendor risk program
- Cyber risk assessments

## PREVENT — Implement safeguards

- Information protection processes & procedures
- Deploy protection technology
- Security controls / logging
- Information backup & DR plan
- Employee training & awareness

## DETECT — Spot cyber events

- Detect anomalies & events
- Continuous monitoring
- Indicators from cyber intelligence team
- Hunt teams (proactive)
- Vulnerability scans & patching

## RESPOND — Mitigate & analyze events

- Analysis
- Mitigation
- Improve
- Communications
- Tabletop exercises

## RECOVER — Process to restore service

- Restore services/capability
- DR/COOP - Recover backups
- Assess program and improve
- Communications to senior leadership & Board

1. Based on NIST Framework for Improving Critical Infrastructure Cybersecurity – https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

# Fraud Schemes and Scams

Bank of America
Merrill Lynch

# Email Fraud

## Social Media

Bad guys rely on social media sites to gather details about a high level executive to impersonate along with a lower-level target.

**Objective: make the target react to the approval power of spoofed executive**

## Domain Change

70% attacks involve domain spoofing[1]

Thieves register a domain that appears similar to the actual domain for a company.

**Objective: the busy target does not notice the fake domain**

## Phishing Email

Recipient receives an email message with his name on it, as well as other details that make it look authentic (relevant details about impersonated executive and likely mentions a specific initiative.)

**Objective: email looks authentic for user to act upon**

## User Assistance

Email looks authentic and prompts for specific action or transaction leading to a loss.

**Objective: create a sense of urgency and may request that the individual bypass normal procedures**

**64% of IT security professionals regard email as a major cyber security threat[1]**
65% don't feel fully equipped or up-to-date to reasonably defend against email based attacks[1]

1. https://www.mimecast.com/resources/press-releases/dates/2016/2/65-percent-of-global-businesses-ill-equipped-to-defend-against-email-based-cyber-attacks/

# Business Email Compromise

## CEO scam

### Phishing Schemes May Involve Mimicking Internal Emails

- Perpetrators know key individuals and their roles in the company based on: information in social media sites, professional associations, company website, etc.
- Domain names may look similar to your company name but are intentionally misspelled
- Fraudulent message appears to be coming from senior executives within the company
- Urgency and confidentiality are key components of the email

Look at the spelling of the words and names *carefully*

CEO@mycompany.com

CEO@rnycompany.com

**From:** Treasurer@mycompany.com
**Sent:** Tuesday, July 8, 2014 11:17a.m.
**To:** chris.smith@mycompany.com
**Subject:** FW: Wire Transfer

This is the third one. We are pulling the confirmation now and will send to you.

**From:** Treasurer@mycompany.com
**Sent:** Wednesday, June 11, 2014 11:30a.m.
**To:** chris.smith@mycompany.com
**Subject:** FW: Wire Transfer

FYI, this needs to get processed today. I checked with (insert name here) to get your help processing it along. I will assume we take care of any vendor forms after the fact. I can send an email directly to (insert name here) or let you drive from here. Let me know.

**From:** Treasurer@mycompany.com
**Sent:** Wednesday, June 11, 2014 9:59a.m.
**To:** chris.smith@mycompany.com
**Subject:** FW: Wire Transfer

Process a wire of $73,508.32 to the attached account information. Code it to admin expense. Let me know when this has been completed.

Thanks.

----------Forwarded message----------

**From:** CEO@rnycompany.com
**Sent:** Wednesday, June 11, 2014 6:45a.m.
**To:** Treasurer@mycompany.com
**Subject:** Wire Transfer

Insert name (Treasurer),

Per our conversation, I have attached the wiring instructions for the wire. Let me know when done.

Thanks. Insert name, (CEO)

# Business Email Compromise

## Vendor email

### Sequence of Events

- Company receives email messages from the “sales person” of their vendor
- Message indicates the vendor is updating their accounts receivable system and changing bank account information
- Company replies to email as well as calls the phone number listed in the email provided for the sales person
- Phone number did not belong to the sales person
- Email address did not belong to the sales person
- Company changed beneficiary account information in AP system
- Payment sent to new beneficiary account
- Vendor notified company of non-receipt of outstanding bill
- Company realized prior emails and phone call was not to the vendor

### Impacts

- Company changed account information in AP system without appropriate verification
- Payment sent to fraudulent beneficiary account
- Vendor notified company of non receipt of outstanding bill
- Company realized emails and phone call were with imposter posing as the vendor

**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

# Best Practices for Business Email Compromise

## Question payment instructions received in email…

Validate using other communication channels

Never reply to the message

Be alert to sudden changes in business practices

Develop procedures for non-standard requests

ALWAYS – Dual approval

## Verify…

- Pick up the phone and call the individual – using the company directory or vendor information Another option is to have another associate create a new email from another PC to validate the instruction
- Validate instructions by having the sender provide the old payment instructions to include beneficiary and account along with the new payment instruction and account – and verify old invoice numbers and dollar amounts
- Ask for the sender to send the new payment instructions from the company letterhead and validate the letterhead
- Ask for a canceled check
- Reach out to vendors – discuss communication of account changes; lay it out in contracts

# Security Best Practices

Bank of America
Merrill Lynch

# Cyber & Fraud Risks

**Protecting against cyber risks & financial fraud** is a top priority for Bank of America Merrill Lynch.

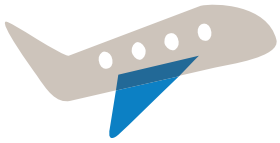
**Passwords**

**Social Engineering**

**Social Media**

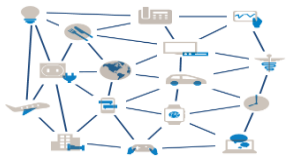
**Mobile & Wireless**

**Travel**



**Ransomware**


**Internet of Things**



**Email**

# Email (BEC)

**Business Email Compromise (BEC)** –Scams target companies of all sizes and personal business transactions by using digital technologies to convince individuals into conducting unauthorized funds transfers

**Reconnaissance** → **Exploitation** → **Delivery** → **Fraud Complete**

- **Reconnaissance**: Criminal utilizes social media to gather intelligence about a firm, high value acquisition and senior executives
- **Exploitation**: Criminal hacks CEO personal email account masquerading as the CEO by spoofing the email identity of the CEO
- **Delivery**: Criminal sends spoofed CEO email about upcoming deal that directs treasury to change funds transfer details
- **Fraud Complete**: Treasury modifies wire transfer - redirects funds to criminal's account

## Vectors of BEC Fraud

- Influence unauthorized account change requests
- Bypass process and request urgent wire transfers
- Email account takeover
- Coerce or trick employee to divulge sensitive financial information

## Considerations

- Follow all processes – verify all exceptions
- Use out-of-band communication channels to verify/confirm change requests
- Be suspicious of unsolicited contact
- When in doubt, stop and verify before acting on requests

# Passwords

**Passwords are the weakest cyber link** – good password management is key to protecting your information and assets.

## Top 10 Easy to Guess Passwords

**Hackers can crack most passwords or already have them from past breaches**[1]

1. 12345
2. Password
3. Football
4. Qwerty
5. Princess
6. Login
7. Welcome
8. Solo
9. Admin
10. password

## Minimum Actions

- **Complexity** – Use a mix of case-sensitive letters, numbers, and special symbols
- **No reuse** – Do not use the same password for multiple accounts
- **2-step & multi-factor** – Use 2-step verification or multi-factor authentication when available
- **Change all defaults** – Change factory default usernames/passwords for new devices (e.g., routers, cameras, smart home devices)

## Additional Considerations

- **No common words**- Avoid common words, phrases, slang, places, or names
- **Acronyms & passphrases** – Acronyms or passphrases (e.g., first letter of each word in a sentence) – memorable but harder to guess
- **Avoid auto-logins** – Storing passwords in macros, log-in scripts or web browsers is risky
- **Password manager** – Generates & stores strong, random passwords; stay organized & secure.

1. https://www.forbes.com/sites/learnvest/2017/02/08/these-are-the-most-hack-able-passwords-out-there-is-yours-one-of-them/#4e735d1d2aef

# Cyber Best Practices

## Recommended Actions

- **Change factory usernames and passwords**
  make them hard to guess
- **Unique passwords for all devices**
  if one is compromised, not all are in jeopardy
- **Install software updates** as soon as possible
- **Do not download unfamiliar software**
- **Use antivirus and anti-malware software**
- **Back up your files regularly**

# Mobile & Wireless

**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**

Enable a passcode, fingerprint or other authentication feature on all mobile devices

**Keep OS & apps updated**

Recent mobile threats targeted devices with unpatched mobile OS & apps. Apply updates as soon as they are available

**Use official app stores**

Apps available via untrusted app stores have a higher risk of malware. Only download from official mobile device vendor and corporate app stores

**Turn off Wi-Fi & Bluetooth if not in use**

Unless needed for a specific purpose, limit access to your location – rogue apps may track you – disable image geo-tagging

**Practice mobile & wireless security** daily to help protect your information and assets

Global wireless carrier networks are more secure than public Wi-Fi. Connect through your carrier when available.

**Connect through a wireless carrier**

When public Wi-Fi is only option, verify name of site Wi-Fi network with staff or posted signage before connecting

**Verify Wi-Fi name before connecting**

When connecting a business device, always use your corporate VPN or other security tools to protect your data

**Connect through corporate VPN**

# Social Media

**Oversharing on Social Media** may expose your sensitive personal or business information - Bad actors may collect your information for cyber attacks and fraud

### Limit Geo-Location Tagging

A common practice is to tag social media posts and photos with your current location. This may reveal too much detail about you, including your home, work, hangout locations you visit. This may put you at risk - consider turning off geo-location tagging unless needed

### Minimum Actions

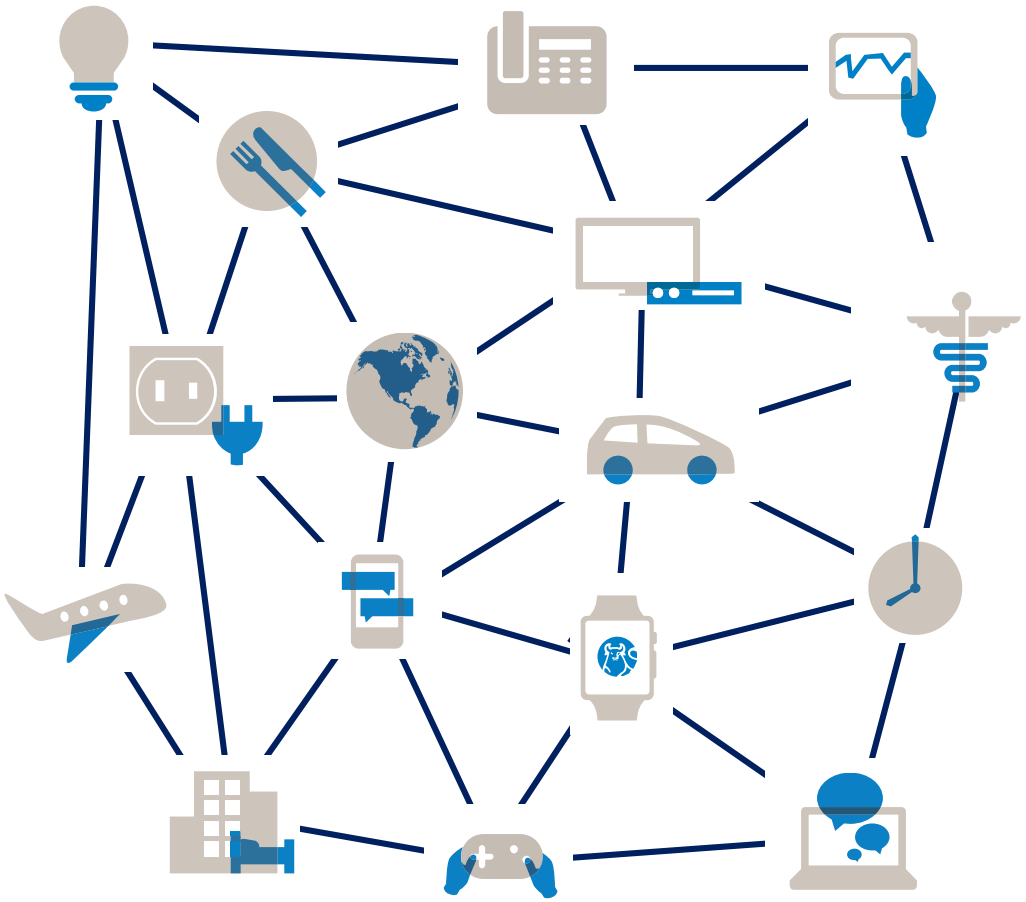
- **Limit what you share** - Anything posted may become public and lives forever, possibly impacting your reputation and future
- **Use caution when accepting new connections** – Cybercriminals create fake profiles and attempt to connect to you
- **Phishing risks** – Cybercriminals are delivering malicious phish to unsuspecting users.
- **Set privacy settings high** - Check your privacy settings to protect your information

### Additional Considerations

- **Scams** – Be aware that advertisements, special offers or news postings may actually be scams to steal information or compromise your account
- **Limit social media apps running in the background** – running mobile apps collect information running in the background.
- **Install apps only from trusted sources** – social media sites offer mobile apps, but criminals may offer fake versions to compromise you

# Internet of Things (IOT)

**The Internet of Things (IoT)** connects machines and devices to each other. IoT and the associate risks are growing exponentially. **By 2020 there may be as many as 50 billion IoT devices[1]**



## Addressing IOT Risks

- Change manufacturer default settings (as defaults are often published on Internet)
- Turn off Internet-enabled features when not in use
- Check privacy settings
- Avoid storing sensitive information on IoT devices
- Update software/firmware
- Be aware of sensitive business or personal conversations near smart assistant devices

Source: CRN Interview with Marc Goodman - https://www.crn.com/news/security/300078161/security-expert-cybercrime-dangers-multiplying-with-rise-of-iot-automation.htm

# Notice to Recipient

"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, capital markets, 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, Merrill Lynch, Pierce, Fenner & Smith Incorporated and Merrill Lynch Professional Clearing Corp., both of which are registered broker-dealers and Members of SIPC, and, in other jurisdictions, locally registered entities. 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.

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 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.

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.

Neither Bank of America nor its affiliates provide information security or information technology (IT) consulting services. This material is provided "as is", with no guarantee of completeness, accuracy, timeliness or of the results obtained from the use of this material, and without warranty of any kind, express or implied, including, but not limited to warranties of performance, quality and fitness for a particular purpose. This material should be regarded as general information on information security and IT considerations and is not intended to provide specific information security or IT advice nor is it any substitute for your own independent investigations. If you have questions regarding your particular IT system or information security concerns, please contact your IT or information security advisor. No information contained herein alters any existing contractual obligations between Bank of America and its clients

Disclaimer for Brazil

Disclaimer for Latin America


Bank of America
Merrill Lynch