CPIM
CENTER FOR PUBLIC INVESTMENT MANAGEMENT

A PROGRAM BY
ROBERT SPRAGUE
OHIO TREASURER

Current Fraud Trends

Business Email Compromise (BEC), Payment Fraud and Paper Check Fraud

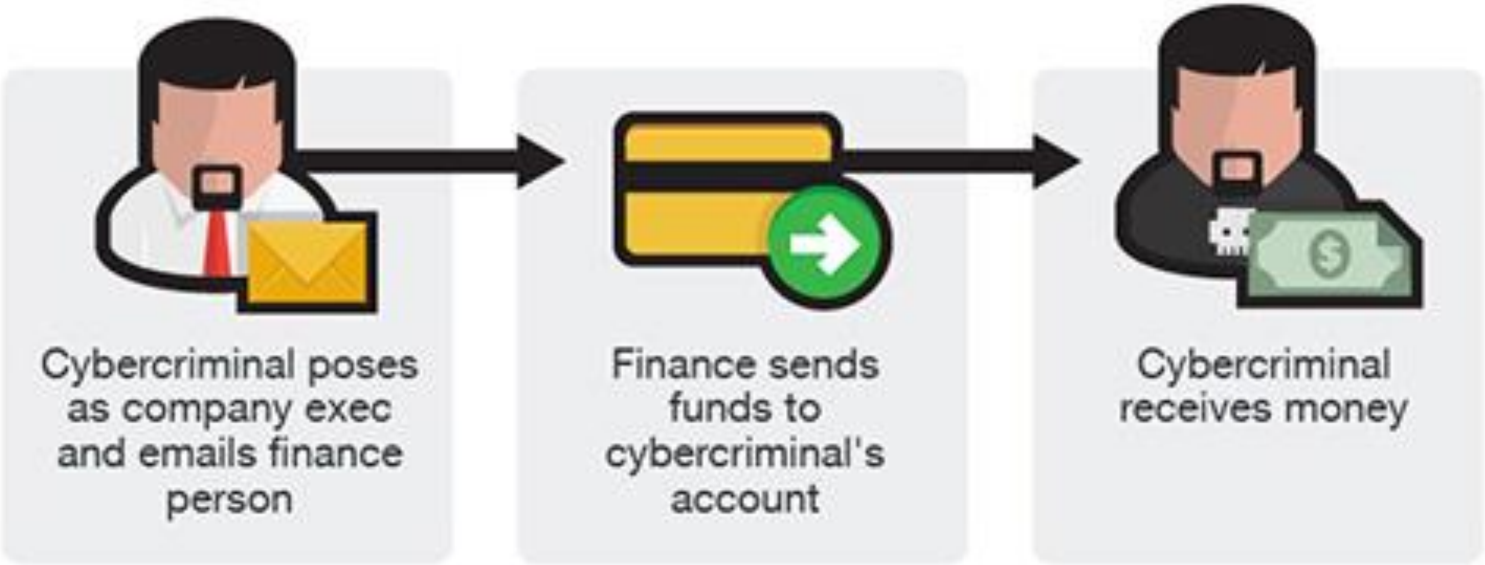
Don Boian, SVP, Security Outreach Director
Huntington National Bank

Agenda

- BEC & Payment Fraud Threats
- BEC & Payment Fraud Best Practices
- Check Fraud
- Detecting Check Fraud
- Q&A

Business E-mail Compromise (BEC)

Fraudulent communications luring employees to take actions which generally results in the movement of funds or disclosure of information



Cybercriminal poses as company exec and emails finance person

Finance sends funds to cybercriminal's account

Cybercriminal receives money

Is it really email <u>compromise</u>?

BEC VS. Phishing

Phishing generally involves the sending of fraudulent e-mails with the intent of luring a user to click a link or open a document, while **BEC** is typically a fraudster spoofing a users email address to send fraudulent emails on their behalf.

Phishing typically results in:

- Compromise of the system: malware or ransomware
- Compromise of credentials: usernames, passwords, etc.

BEC typically results in:

- Disclosure of sensitive and/or personal information
- Movement of funds

BEC prevention training shares the common safeguards used with anti-phishing education courses

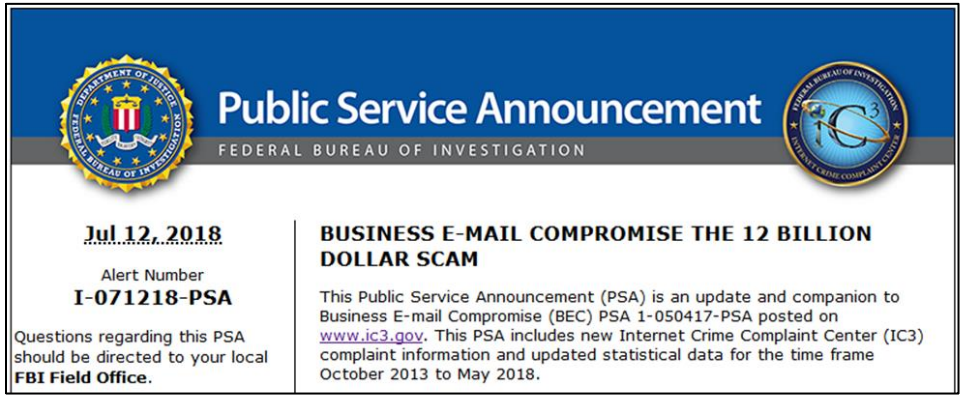
BEC on the Rise

The FBI estimates that actual and intended losses from business email compromise have increased by more than **2,000 %** since late 2013

$12.5 Billion

October 2013 - May 2018

$2.9B in the US


Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

Jul 12, 2018

Alert Number

I-071218-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office.**

BUSINESS E-MAIL COMPROMISE THE 12 BILLION DOLLAR SCAM

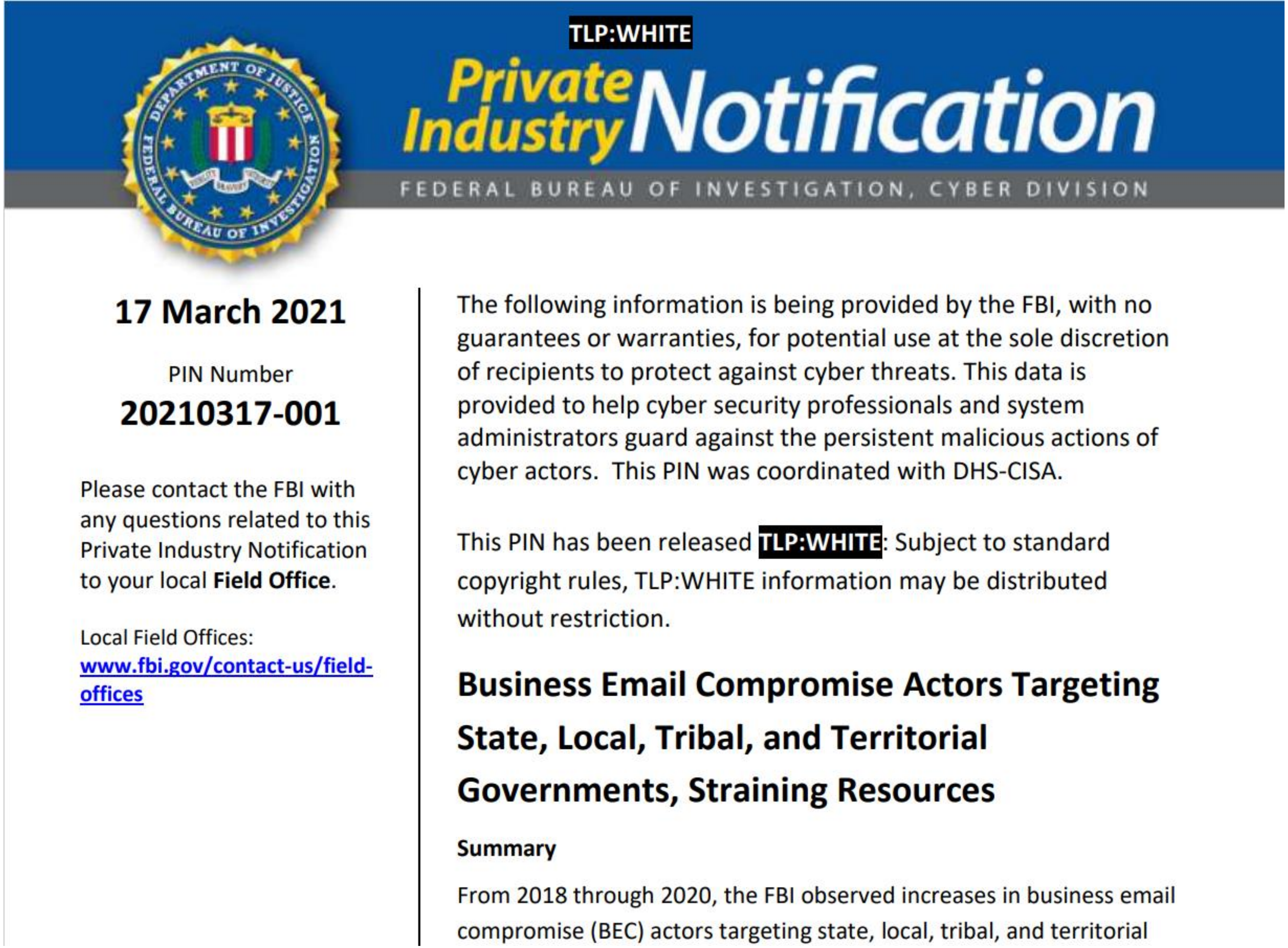
This Public Service Announcement (PSA) is an update and companion to Business E-mail Compromise (BEC) PSA 1-050417-PSA posted on www.ic3.gov. This PSA includes new Internet Crime Complaint Center (IC3) complaint information and updated statistical data for the time frame October 2013 to May 2018.

According to the FBI, a rise in BEC associated with to the COVID-19 pandemic is anticipated, however some progress has been made on pursuing the fraudsters

2020 – 19,369 BEC Complaints

$1.8 Billion in losses

Source: FBI Alert Number I-071218-PSA (https://www.ic3.gov/media/2018/180712.aspx)
https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf



TLP:WHITE

Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

17 March 2021

PIN Number

20210317-001

Please contact the FBI with any questions related to this Private Industry Notification to your local **Field Office**.

Local Field Offices: www.fbi.gov/contact-us/field-offices

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients to protect against cyber threats. This data is provided to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber actors. This PIN was coordinated with DHS-CISA.

This PIN has been released TLP:WHITE: Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

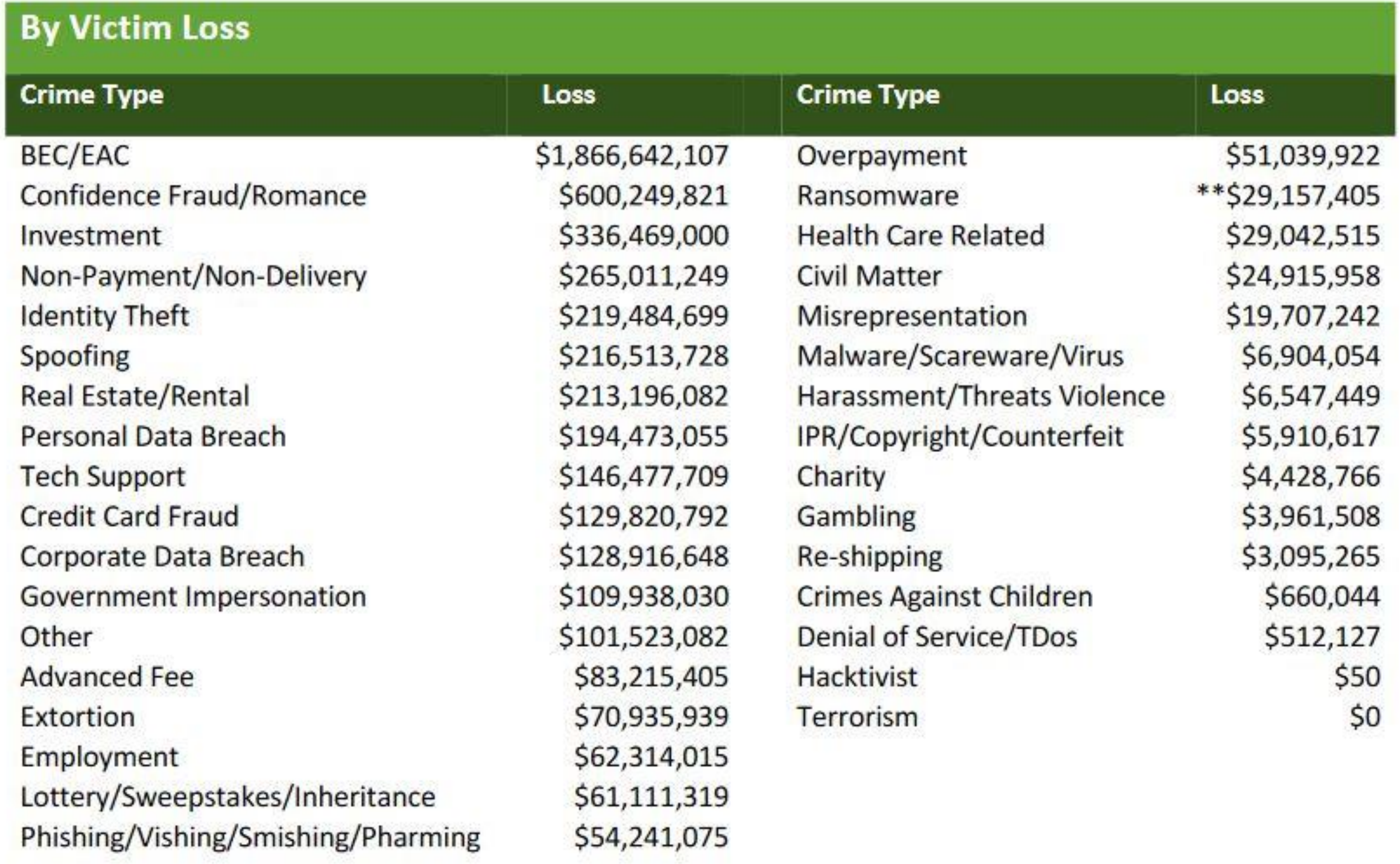
Business Email Compromise Actors Targeting State, Local, Tribal, and Territorial Governments, Straining Resources

Summary

From 2018 through 2020, the FBI observed increases in business email compromise (BEC) actors targeting state, local, tribal, and territorial

Source: [Business Email Compromise Actors Targeting State, Local, Tribal, and Territorial Governments, Straining Resources (ic3.gov)](ic3.gov)

2020 Crime Types *Continued*



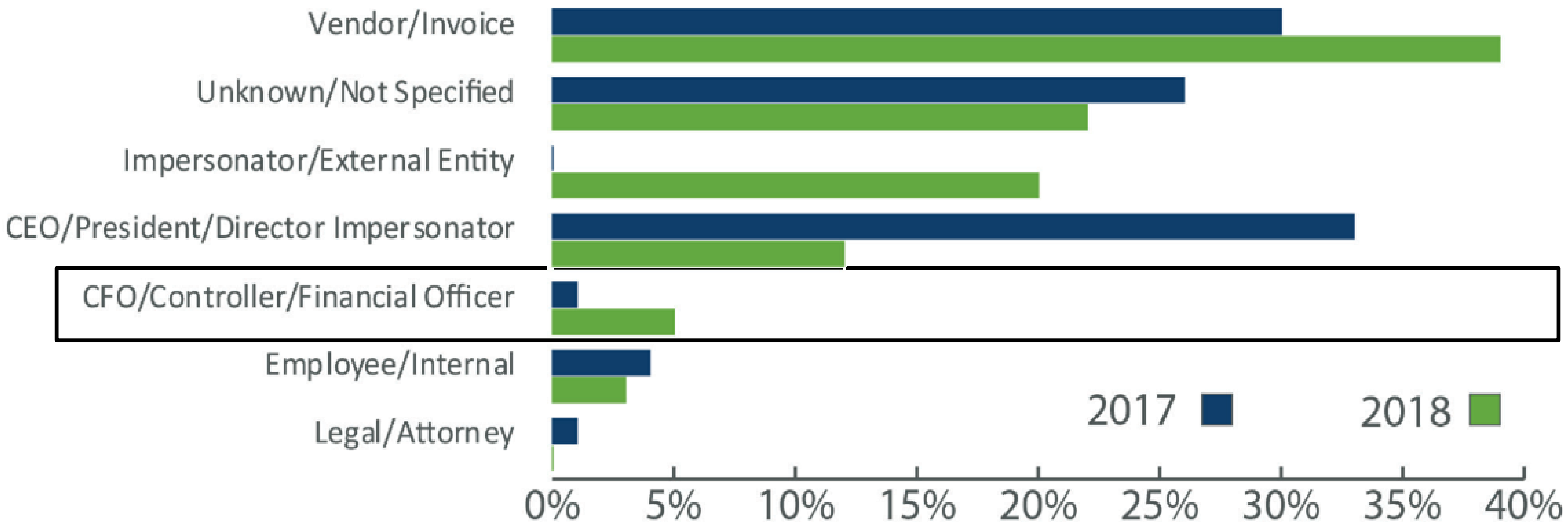
By Victim Loss

Crime Type	Loss	Crime Type	Loss
BEC/EAC	$1,866,642,107	Overpayment	$51,039,922
Confidence Fraud/Romance	$600,249,821	Ransomware	**$29,157,405
Investment	$336,469,000	Health Care Related	$29,042,515
Non-Payment/Non-Delivery	$265,011,249	Civil Matter	$24,915,958
Identity Theft	$219,484,699	Misrepresentation	$19,707,242
Spoofing	$216,513,728	Malware/Scareware/Virus	$6,904,054
Real Estate/Rental	$213,196,082	Harassment/Threats Violence	$6,547,449
Personal Data Breach	$194,473,055	IPR/Copyright/Counterfeit	$5,910,617
Tech Support	$146,477,709	Charity	$4,428,766
Credit Card Fraud	$129,820,792	Gambling	$3,961,508
Corporate Data Breach	$128,916,648	Re-shipping	$3,095,265
Government Impersonation	$109,938,030	Crimes Against Children	$660,044
Other	$101,523,082	Denial of Service/TDos	$512,127
Advanced Fee	$83,215,405	Hacktivist	$50
Extortion	$70,935,939	Terrorism	$0
Employment	$62,314,015		
Lottery/Sweepstakes/Inheritance	$61,111,319		
Phishing/Vishing/Smishing/Pharming	$54,241,075		

Source: 2020_IC3Report.pdf
Almost $2 billion lost to BEC scams in 2020 | WeLiveSecurity

Business E-mail Compromise

2017 & 2018 BEC Identified Scams



Source: https://www.fincen.gov/sites/default/files/shared/FinCEN_Financial_Trend_Analysis_FINAL_508.pdf

BEC Tactics

- Sense of urgency
- Timing – often near close of business on Friday
- Use of current crisis as topic or to increase urgency
- Increase in target development and sophistication
  - Gathering intelligence
  - Open source, social media
  - Social Engineering

Source: https://www.bankinfosecurity.com/bec-campaign-targets-hr-departments-report-a-13997
https://www.databreachtoday.com/ta505-apt-group-returns-new-techniques-report-a-13678

BEC Case Study

Invoicing

BEC: Invoicing

Construction invoicing (St. Ambrose Catholic Parish)

1. Parish email server compromised
2. Fraudsters monitor communications
3. Valid invoice submitted to parish for payment
4. fraudster spoofs message, as construction firm, to parish requesting a change in payment wire instructions

$1.75M LOST

Source: https://threatpost.com/bec-hack-cons-catholic-church/144212/
https://www.cleveland.com/crime/2019/04/email-hackers-steal-175-million-from-st-ambrose-catholic-parish-in-brunswick.html
https://www.news5cleveland.com/news/local-news/oh-cuyahoga/saint-ambrose-catholic-parish-victim-of-sophisticated-business-email-scheme-fbi-says
https://www.scmagazine.com/home/security-news/cybercrime/st-ambrose-catholic-parish-in-brunswick-ohio-was-hit-with-a-business-email-compromise-scam/

BEC Case Study

Payment Fraud

Huntington
Welcome.

Peterborough, NH – August 2021

- Email impersonating local school district demands $1.2M monthly payment
- Investigation discovered other fraudulent payments
- Erroneous payments ($1.1M) meant for a construction firm working on bridge repair
- Secret Service investigation shows that the money was laundered through cryptocurrency

Total loss: $2.3M

Source: New Hampshire town lost $2.3 million in email scam (statescoop.com)
FBI: State and Local Governments Losing Millions to BEC - Infosecurity Magazine (infosecurity-magazine.com)

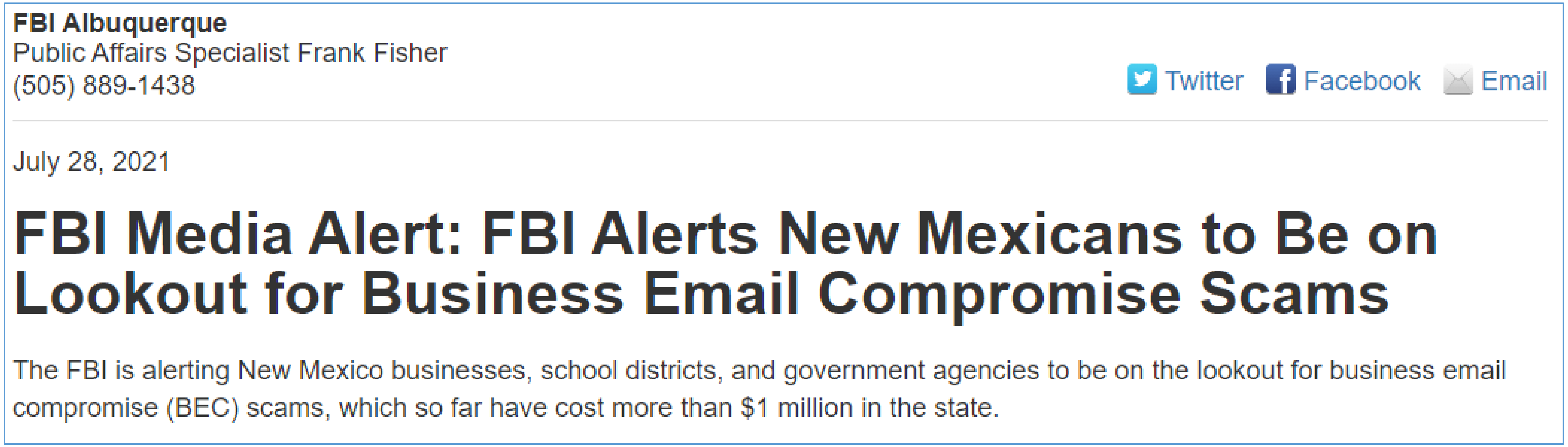
BEC Case Study

Payment Fraud

Huntington
Welcome.

New Mexico – July 2021

- BEC fraudsters targeting businesses, school districts and government agencies



FBI Albuquerque
Public Affairs Specialist Frank Fisher
(505) 889-1438

July 28, 2021

FBI Media Alert: FBI Alerts New Mexicans to Be on Lookout for Business Email Compromise Scams

The FBI is alerting New Mexico businesses, school districts, and government agencies to be on the lookout for business email compromise (BEC) scams, which so far have cost more than $1 million in the state.

Total loss: $1.025M (Jan-Jun)

Source: FBI alerts New Mexico businesses, schools, govt. of email scams (deminghеadlight.com)
FBI Media Alert: FBI Alerts New Mexicans to Be on Lookout for Business Email Compromise Scams — FBI

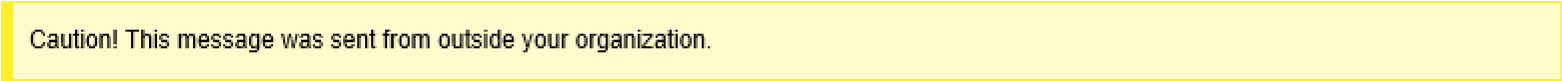
Reducing the Risk of Business Email Compromise (BEC) Best Practices

Huntington
Welcome.

Detecting BEC - Red Flags:

The E-mail Bait

- E-mail address variation (user or domain name)
- Misspelling
- Sense of urgency in the request
- Change in email tone
- Removal of addressees on the email chain (cc or other addresses)



Caution! This message was sent from outside your organization.

Detecting BEC - Red Flags:

Procedural Clues

- Requests outside of normal procedures
- Change in payment instructions
- Change in vendor
- Changes to phone number
- Beneficiary changes (from account to account)
- Name/Account mismatch; Returned wires

Know your customer

- If client phone is never answered or goes directly to VM
- Cultural changes/differences; Changes in customer behavior

Know your suppliers

Best Practices:

People

- Educate your employees – Share BEC threats and scams
- Limit publicly available information
  - Contact, organizational structure, process info

Process

- Well documented processes; Periodically reviewed/updated
- Evaluate all processes for potential fraud trouble spots
- Implement multiple controls
  - Call back procedures for verification (e.g. payment change)
  - Voice Approval
  - Use phone numbers that are on file (not passed in email) for call back
  - Dual authorization – look out for each other!

Technology

- Independent assessment or “Red team” all processes/controls
- Report and save all emails of suspected BEC
- Use two-factor authentication on accounts that support it. Never disable it
- Disable or monitor the use of email auto-forward
- Protect your brand/domain – monitor for spoofed domain; Implement DMARC, BIMI

Source: https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/business-email-compromise

Cybersecurity Liability Insurance

Cybersecurity Liability Insurance generally covers losses resulting from data breaches and cybersecurity incidents/events

First Party Coverage

- Loss or Damage of Electronic Data
- Loss of income/expenses
- Cyber Extortion (got bitcoin?)
- Notification Costs
- Repair damaged SW & HW
- Consumer credit monitoring
- Cyber Crime

Third Party Coverage

- Network Security & Privacy Liability
- Electronic Media Liability
- Regulatory Proceedings
- Breach of contract/Negligence

Know Your Policy Coverage and Limitations

- Does it cover:
  - System Failure
  - Bricking
  - Betterment
  - Social Engineering & Invoice Manipulation
- Have you reviewed your contracts with 3rd parties to identify cyber insurance requirements or any limitations of liability?
- **Have a trained professional go over your current policy!**

What to do if you suspect BEC

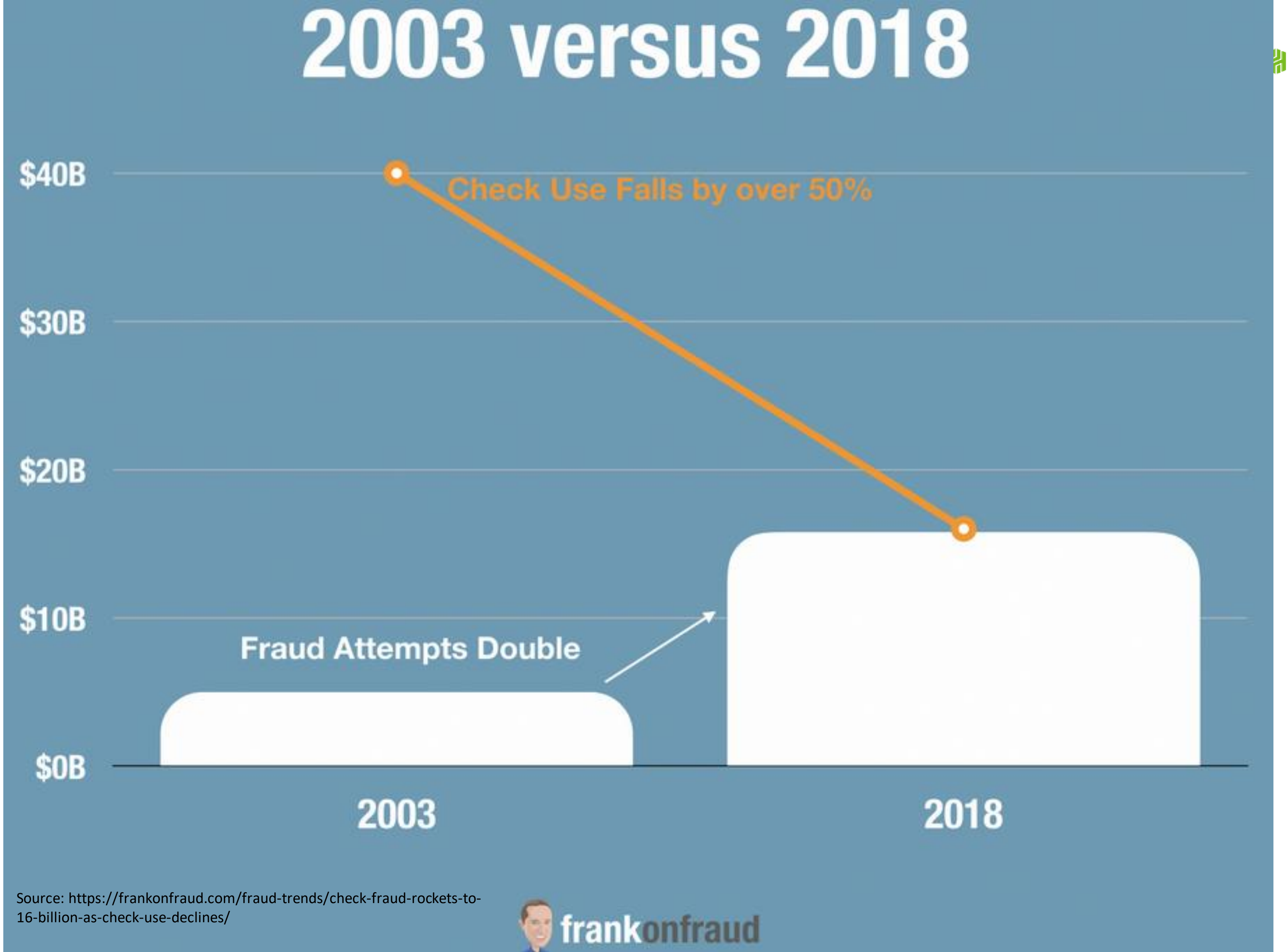
If you or your company fall victim to a BEC scam, it’s important to act quickly:

- Contact your financial institution immediately to request that they contact the financial institution where the transfer was sent.
- Report the crime to your FBI Field Office.
- File a complaint with the FBI’s Internet Crime Complaint Center.
- Contact your Cybersecurity Insurance Carrier and engage forensic and remediation services

Source: https://www.fbi.gov/contact-us/field-offices
https://www.ic3.gov/default.aspx

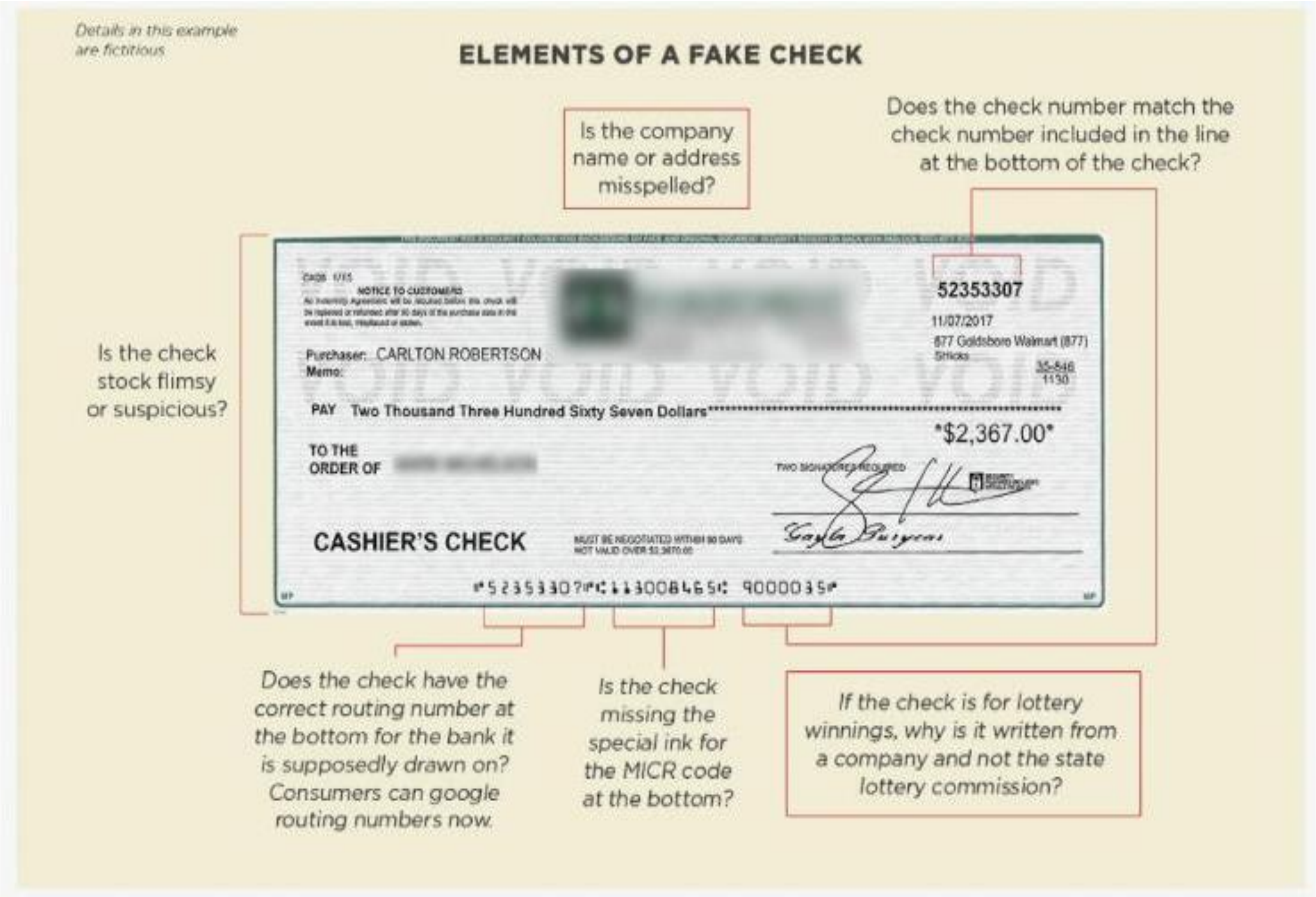
Check Fraud

Huntington
Welcome.



Source: https://frankonfraud.com/fraud-trends/check-fraud-rockets-to-16-billion-as-check-use-declines/

Spotting Fraudulent Checks



Details in this example are fictitious

ELEMENTS OF A FAKE CHECK

Is the company name or address misspelled?

Does the check number match the check number included in the line at the bottom of the check?

Is the check stock flimsy or suspicious?

NOTICE TO CUSTOMERS

[redacted]

52353307

11/07/2017

877 Goldsboro Walmart (877)
Sticks

35-846
1130

Purchaser: CARLTON ROBERTSON
Memo:

PAY Two Thousand Three Hundred Sixty Seven Dollars***

$2,367.00

TO THE ORDER OF [redacted]

TWO SIGNATURES REQUIRED

CASHIER'S CHECK

MUST BE NEGOTIATED WITHIN 90 DAYS
NOT VALID OVER $2,3670.00

⑈52353307⑈ ⑆113008465⑆ 9000035⑈

Does the check have the correct routing number at the bottom for the bank it is supposedly drawn on? Consumers can google routing numbers now.

Is the check missing the special ink for the MICR code at the bottom?

If the check is for lottery winnings, why is it written from a company and not the state lottery commission?

Source: https://www.bbb.org/article/news-releases/18367-dont-cash-that-check-bbb-study-shows-how-fake-check-scams-bait-consumers

Spotting Fraudulent Checks

- Misspelling
- Numerical amount does not match written amount
- Change or variations in font or text size (Payee address, legal line, Pay to line)
- Pay to the Order of ********* or includes the word “Attention” before payee
- Unaligned Text
- Changes to Routing or Account Numbers
- Improper endorsement
- MICR Ink is missing or appears altered/shiny
- Watermarks appear altered or are missing
- Images that should be holograms or reflective are not
- Misplaced, missing or blurred images (business logos)
- Microprinting appears as a solid line
- Geographic differences – signatory in State A, payee in State B or not in region
- Cashier’ checks, official checks and/or money orders require additional scrutiny as they are commonly counterfeited

Source: https://www.bbb.org/article/news-releases/18367-dont-cash-that-check-bbb-study-shows-how-fake-check-scams-bait-consumers

Q&A

Appendix

Huntington
Welcome.

Resources

National Automated Clearing House Association:

https://www.nacha.org/case-studies/business-email-compromise-and-vendor-impersonation-fraud-what-you-need-know

FBI:

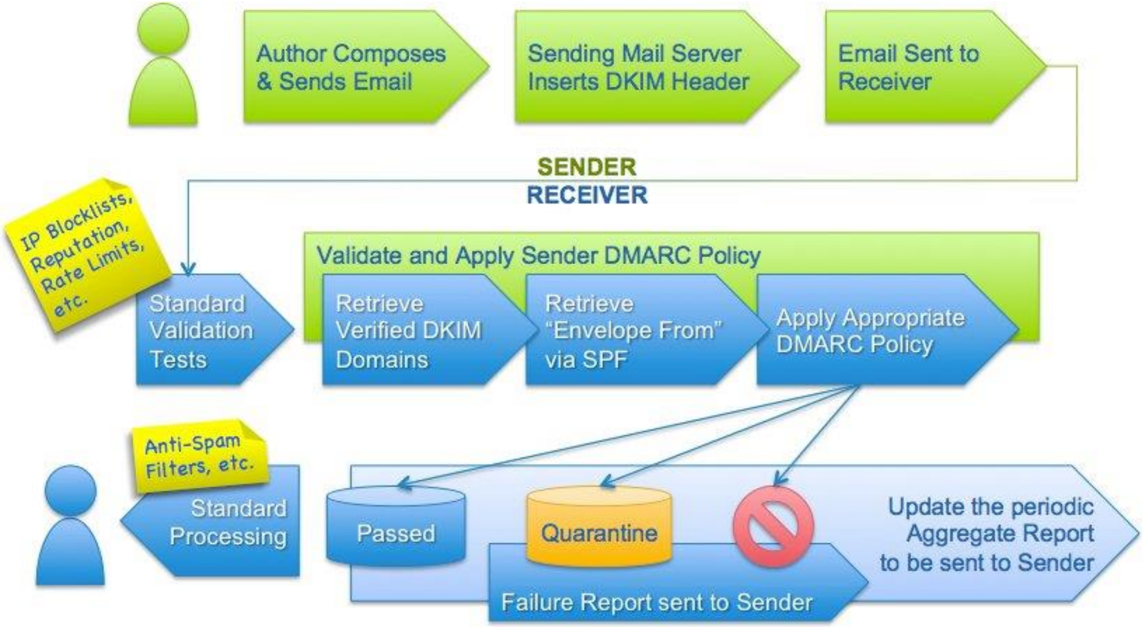
https://www.fbi.gov/news/stories/business-e-mail-compromise-on-the-rise

FBI Internet Crime Complaint Center (IC3):

https://www.ic3.gov/default.aspx

Implement Domain Message Authentication Reporting & Conformance (DMARC)

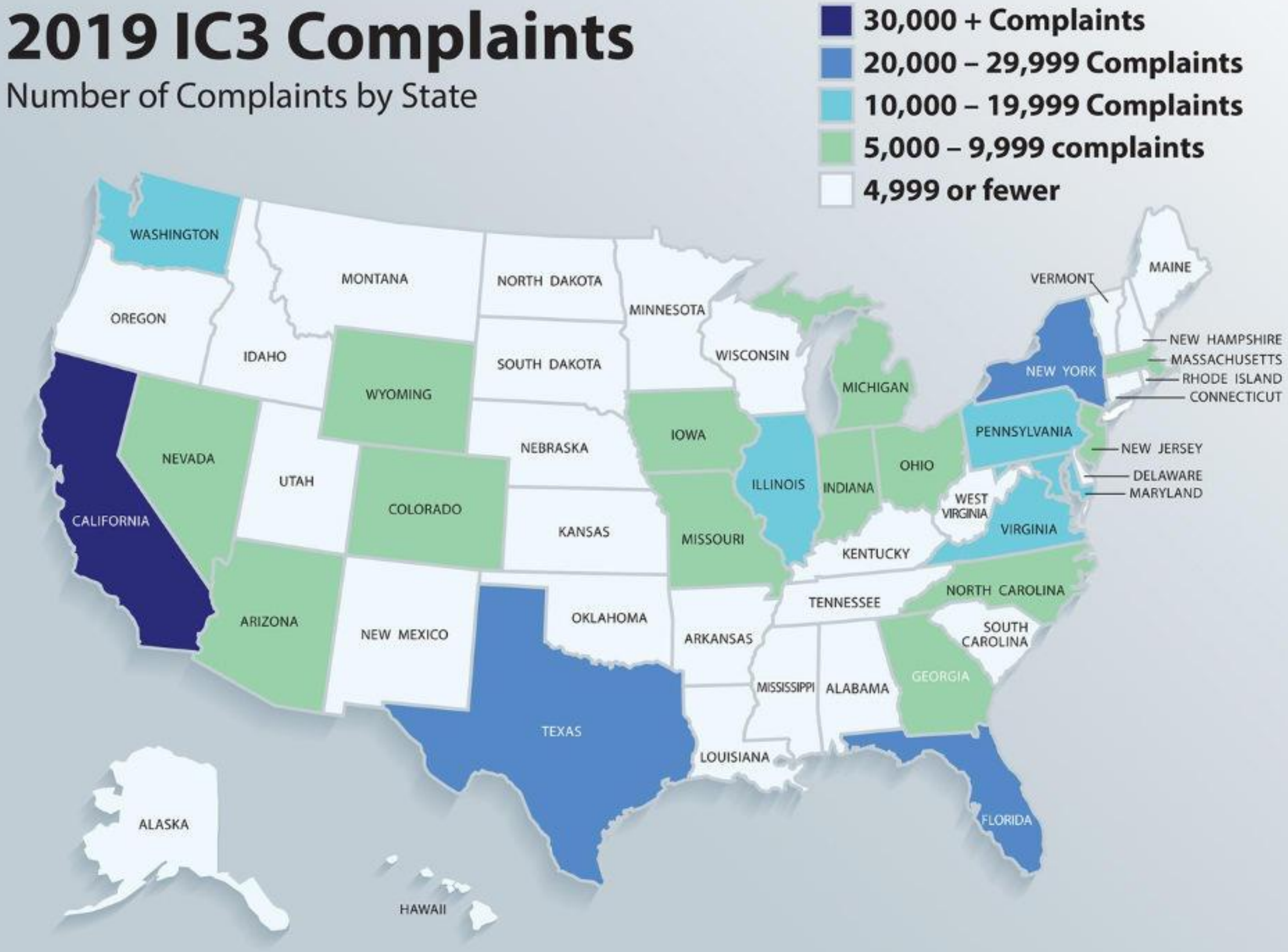
- Builds on Sender Policy Framework (SPF) and Domain Keys Identified Message (DKIM) protocols
- Brand Indicators for Message Identification (BIMI) – YOUR logo on YOUR emails


Author Composes & Sends Email
Sending Mail Server Inserts DKIM Header
Email Sent to Receiver
SENDER
RECEIVER
IP Blocklists, Reputation, Rate Limits, etc.
Validate and Apply Sender DMARC Policy
Standard Validation Tests
Retrieve Verified DKIM Domains
Retrieve "Envelope From" via SPF
Apply Appropriate DMARC Policy
Anti-Spam Filters, etc.
Standard Processing
Passed
Quarantine
Update the periodic Aggregate Report to be sent to Sender
Failure Report sent to Sender

Source: https://dmarc.org/
https://bimigroup.org/

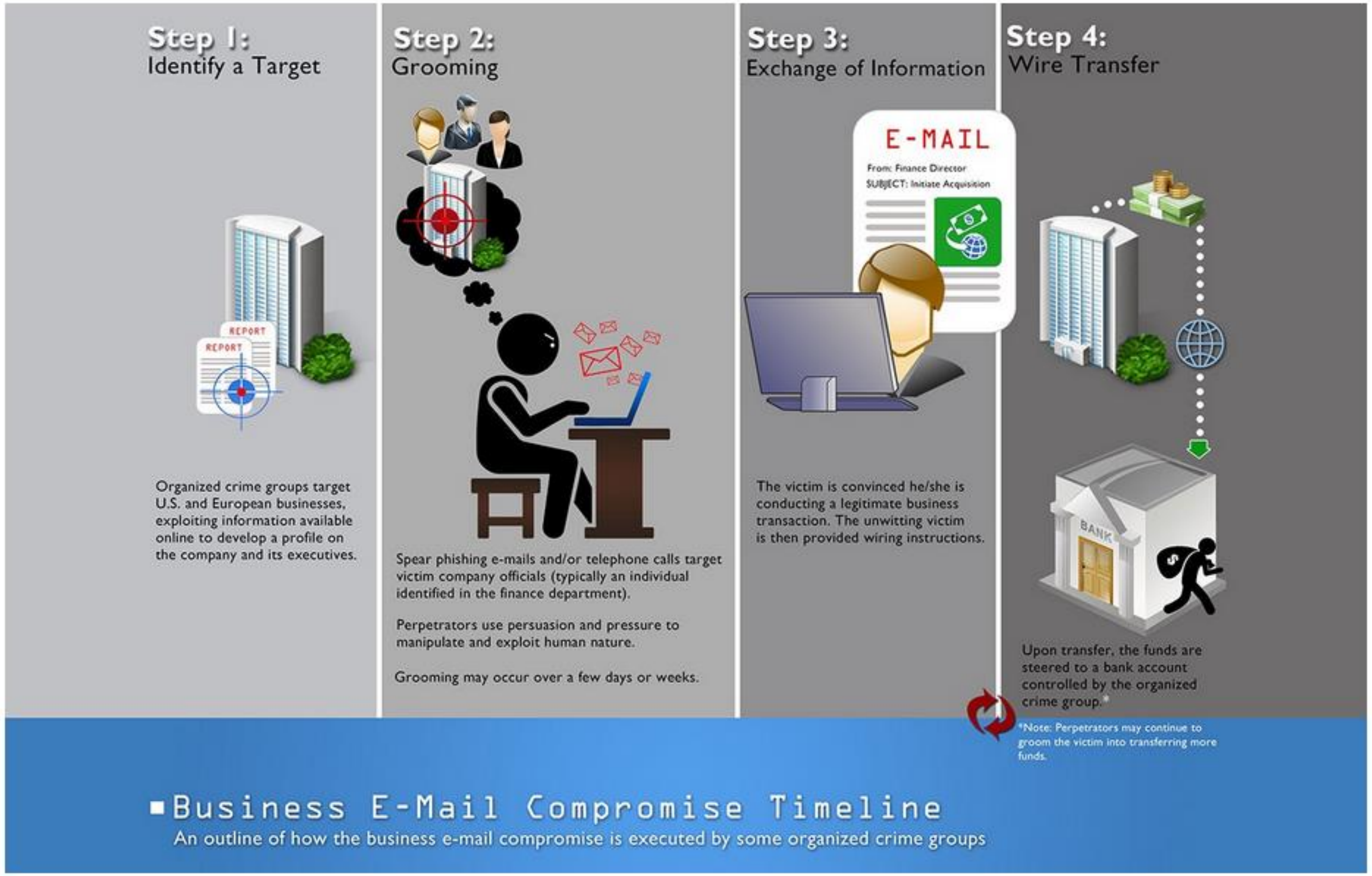
2019 IC3 Complaints

Number of Complaints by State



Source: 2019 Internet Crime Report

Source: https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120



Step 1: Identify a Target

Organized crime groups target U.S. and European businesses, exploiting information available online to develop a profile on the company and its executives.

Step 2: Grooming

Spear phishing e-mails and/or telephone calls target victim company officials (typically an individual identified in the finance department).

Perpetrators use persuasion and pressure to manipulate and exploit human nature.

Grooming may occur over a few days or weeks.

Step 3: Exchange of Information

The victim is convinced he/she is conducting a legitimate business transaction. The unwitting victim is then provided wiring instructions.

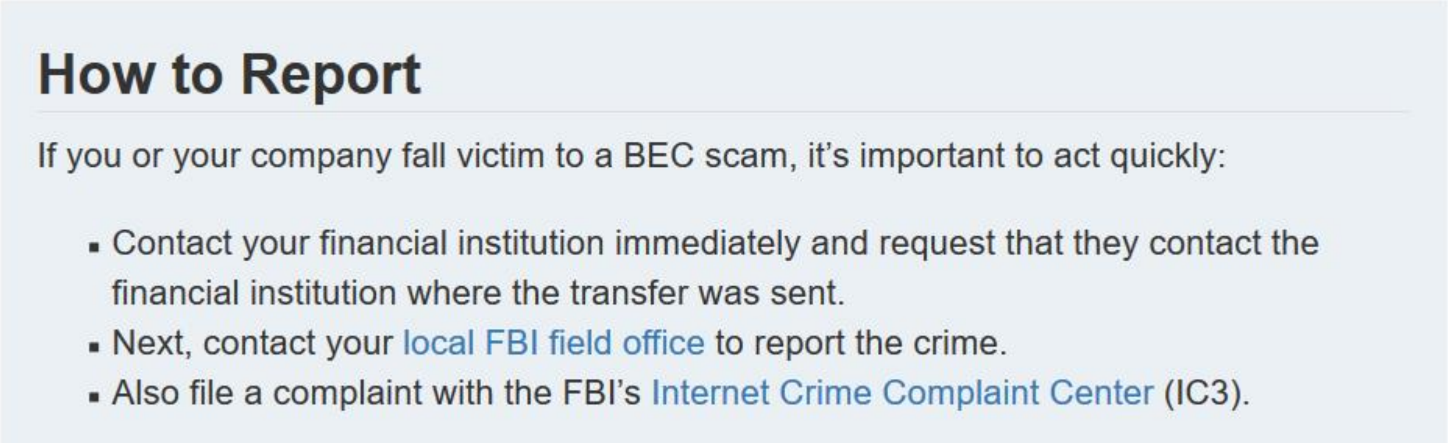
Step 4: Wire Transfer

Upon transfer, the funds are steered to a bank account controlled by the organized crime group.*

*Note: Perpetrators may continue to groom the victim into transferring more funds.

■ Business E-Mail Compromise Timeline

An outline of how the business e-mail compromise is executed by some organized crime groups



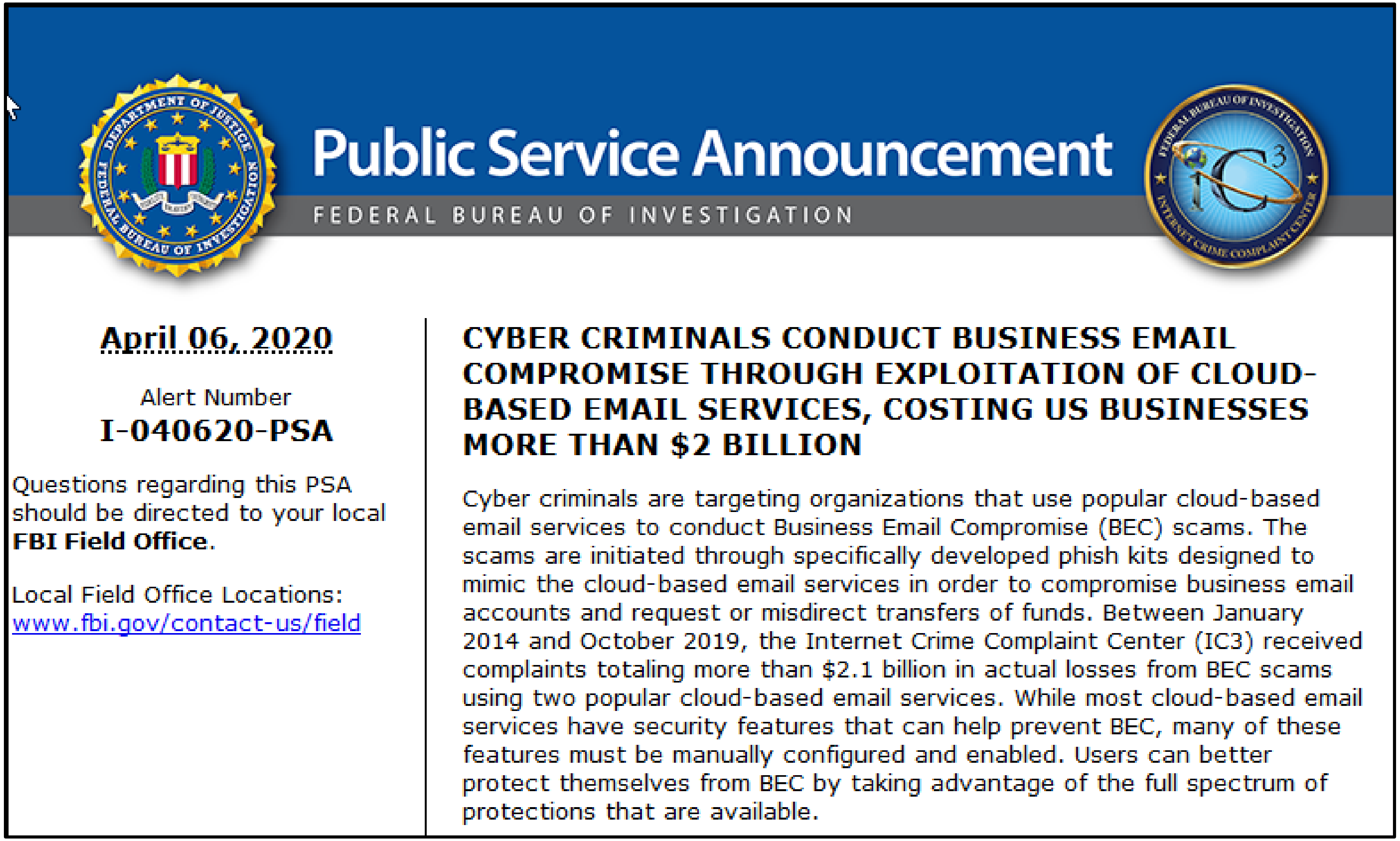
How to Report

If you or your company fall victim to a BEC scam, it's important to act quickly:

- Contact your financial institution immediately and request that they contact the financial institution where the transfer was sent.
- Next, contact your local FBI field office to report the crime.
- Also file a complaint with the FBI's Internet Crime Complaint Center (IC3).

Source: https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/business-email-compromise

FBI PSA



Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

April 06, 2020

Alert Number
I-040620-PSA

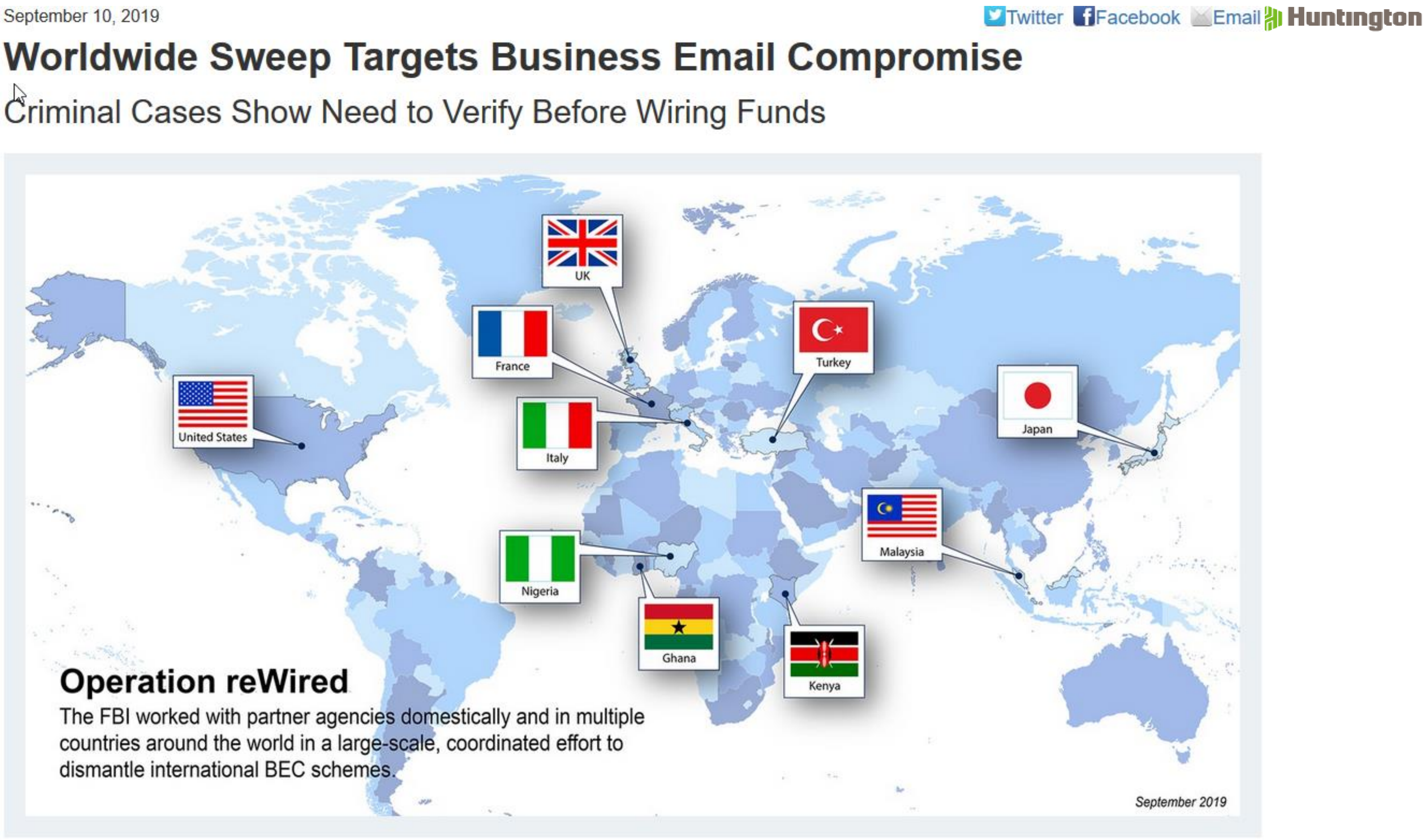
Questions regarding this PSA should be directed to your local **FBI Field Office**.

Local Field Office Locations:
www.fbi.gov/contact-us/field

CYBER CRIMINALS CONDUCT BUSINESS EMAIL COMPROMISE THROUGH EXPLOITATION OF CLOUD-BASED EMAIL SERVICES, COSTING US BUSINESSES MORE THAN $2 BILLION

Cyber criminals are targeting organizations that use popular cloud-based email services to conduct Business Email Compromise (BEC) scams. The scams are initiated through specifically developed phish kits designed to mimic the cloud-based email services in order to compromise business email accounts and request or misdirect transfers of funds. Between January 2014 and October 2019, the Internet Crime Complaint Center (IC3) received complaints totaling more than $2.1 billion in actual losses from BEC scams using two popular cloud-based email services. While most cloud-based email services have security features that can help prevent BEC, many of these features must be manually configured and enabled. Users can better protect themselves from BEC by taking advantage of the full spectrum of protections that are available.

Source: https://www.ic3.gov/media/2020/200406.aspx



September 10, 2019

Worldwide Sweep Targets Business Email Compromise

Criminal Cases Show Need to Verify Before Wiring Funds

Operation reWired

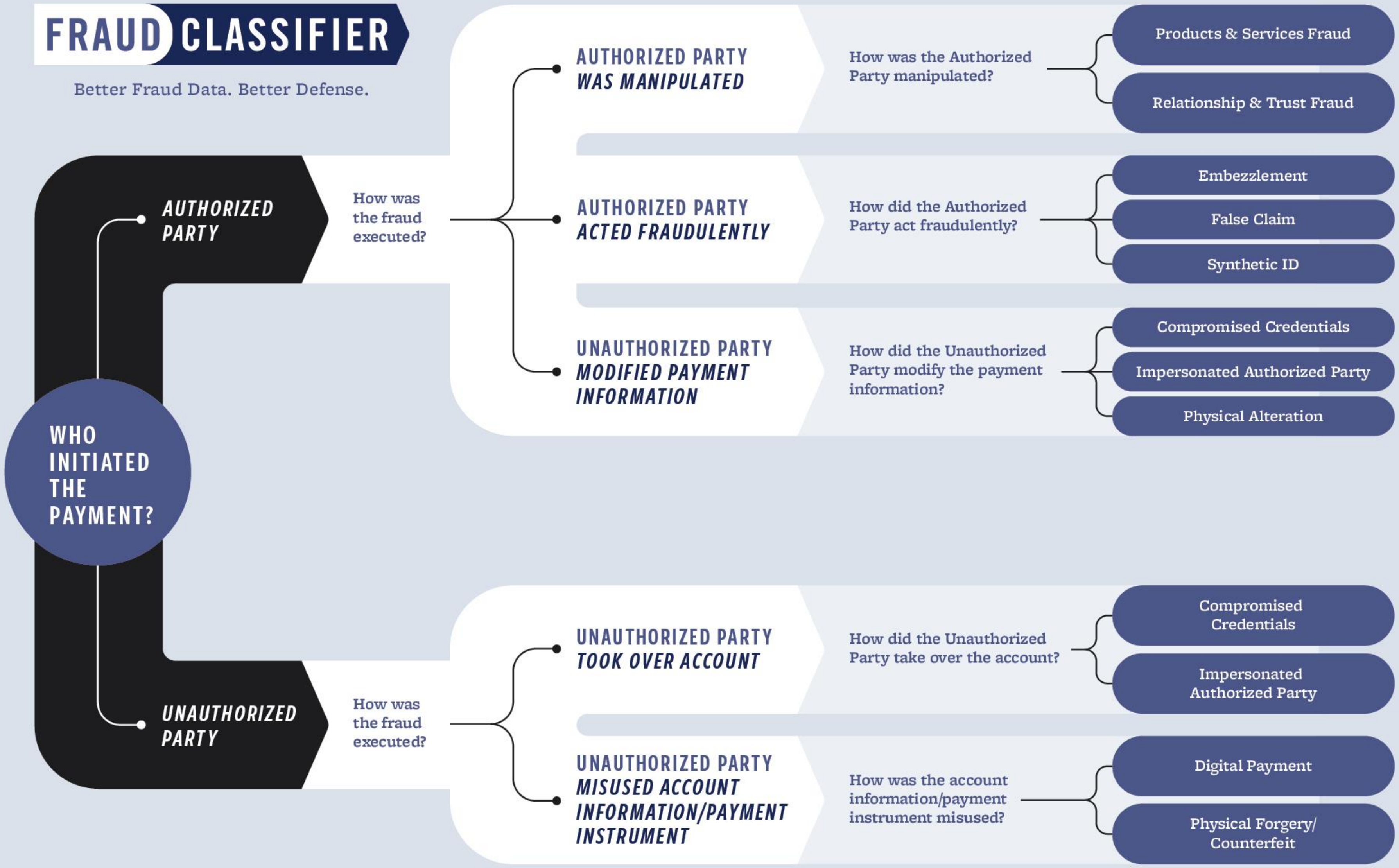
The FBI worked with partner agencies domestically and in multiple countries around the world in a large-scale, coordinated effort to dismantle international BEC schemes.

September 2019

Source: https://www.fbi.gov/news/stories/operation-rewired-bec-takedown-091019

FRAUD CLASSIFIER

Better Fraud Data. Better Defense.



WHO INITIATED THE PAYMENT?

AUTHORIZED PARTY — How was the fraud executed?

- AUTHORIZED PARTY WAS MANIPULATED — How was the Authorized Party manipulated?
  - Products & Services Fraud
  - Relationship & Trust Fraud
- AUTHORIZED PARTY ACTED FRAUDULENTLY — How did the Authorized Party act fraudulently?
  - Embezzlement
  - False Claim
  - Synthetic ID
- UNAUTHORIZED PARTY MODIFIED PAYMENT INFORMATION — How did the Unauthorized Party modify the payment information?
  - Compromised Credentials
  - Impersonated Authorized Party
  - Physical Alteration

UNAUTHORIZED PARTY — How was the fraud executed?

- UNAUTHORIZED PARTY TOOK OVER ACCOUNT — How did the Unauthorized Party take over the account?
  - Compromised Credentials
  - Impersonated Authorized Party
- UNAUTHORIZED PARTY MISUSED ACCOUNT INFORMATION/PAYMENT INSTRUMENT — How was the account information/payment instrument misused?
  - Digital Payment
  - Physical Forgery/ Counterfeit

The FraudClassifier℠ model was developed by a cross-industry work group to provide a consistent way to classify and understand how fraud occurs across the payments industry. The FraudClassifier model is not intended to result in mandates or regulations, and does not give any legal status, rights or responsibilities, nor is it intended to define or imply liabilities for fraud loss or create legal definitions, regulatory or reporting requirements. While sharing and use of the FraudClassifier model throughout the industry is encouraged, any adoption of the FraudClassifier model is voluntary at the discretion of each individual entity. Absent written consent, the FraudClassifier model may not be used in a manner that suggests the Federal Reserve endorses a third-party product or service.

Source: https://fedpaymentsimprovement.org/strategic-initiatives/payments-security/fraudclassifier-model/

Personal Cybersecurity Basics*

1. Raise awareness (Phishing, Social Engineering, …) – know the threats
2. Passwords – NO reuse; Complex; Passphrase; Use a Password Manager
3. Backup data
4. Updated/Current OS and Applications – allow auto-update
5. Antivirus, Firewall, Home network – change default passwords!
6. Terms of Service; Beware of free services – YOU'RE the product
7. Geolocation/Location based services
8. Reputable applications and what they have access to
9. Home IoT Devices – Change default passwords; Security
10. WiFi Security
11. Credit Cards – Transaction Alerts (CNP); Use mobile app locking
12. Credit Reporting Bureaus - Freeze/Lock credit
13. Application Settings - Security & Privacy – periodically review/reset

- **BE BRILLANT AT THE BASICS**

* Start with these, but don't stop there once you've mastered them

References

- Huntington - Privacy & Security
  - https://www.huntington.com/Privacy-Security
- FBI
  - Internet Crime Complaint Center (IC3)
    - https://www.ic3.gov/default.aspx
  - Public Service Announcements
    - https://www.ic3.gov/media/default.aspx
- Federal Trade Commission –
  - Cybersecurity for Small Business
    - https://www.ftc.gov/tips-advice/business-center/small-busines curity
  - Identity Theft
    - http://www.identitytheft.gov/
- NIST Cybersecurity Framework
  - https://www.nist.gov/cyberframework/framework
- Center for Internet Security
  - https://www.cisecurity.org/
- Cloud Security Alliance
  - https://cloudsecurityalliance.org/

References

- Credit Reporting Agencies
  - Equifax (888)766-0008 http://www.equifax.com/CreditReportAssistance
  - Experian (888)397-3742
    - Fraud - https://www.experian.com/fraud
    - Freeze - https://www.experian.com/freeze/center.html
  - TransUnion (800)680-7289
    - Fraud – https://www.transunion.com/solution/fraud-detection
    - Freeze - https://www.transunion.com/blog/identity-protection/credit-freeze-vs-credit-lock
- Federal Trade Commission – Complaint
  - http://www.ftc.gov/complaint

References – Cybersecurity Careers & Education

- Careers in Cybersecurity – CyberSeek
  - https://www.cyberseek.org/heatmap.html
  - https://www.cyberseek.org/pathway.html
- National Institute of Standards and Technology (NIST)

  National Initiative for Cybersecurity Education (NICE) Framework
  - https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework
- National Initiative for Cybersecurity Careers and Studies (NICCS)
  - https://niccs.us-cert.gov/
- STOP. THINK. CONNECT.
  - https://www.stopthinkconnect.org/
- FBI – Safe Online Surfing
  - https://sos.fbi.gov/en/