

Mitigating Loss: Combating the True Cost of Fraud

Terri Luttrell, CAMS-Audit, CFCS
April 2024

Fraud Trends

Top scams of 2023

- Imposter scams
- Online Shopping
- Prizes, sweepstakes, lotteries
- Investment scams
- Business and job opportunities

Business and investment fraud

Business and investment fraud

- **Business email compromise (BEC):** Criminals send email message that appears to come from a known source
- **Advance fee schemes:** Investors are asked to pay a fee upfront for an investment deal to go through
- **Nigerian letter (419 fraud):** Sender requests help facilitating the illegal transfer of money to get funds out of Nigeria
- **Ponzi schemes:** Use current investors' money to pay previous investors
- **Pyramid schemes:** Asks the investor to bring in new investors to make a profit or recoup their investment



Consumer fraud

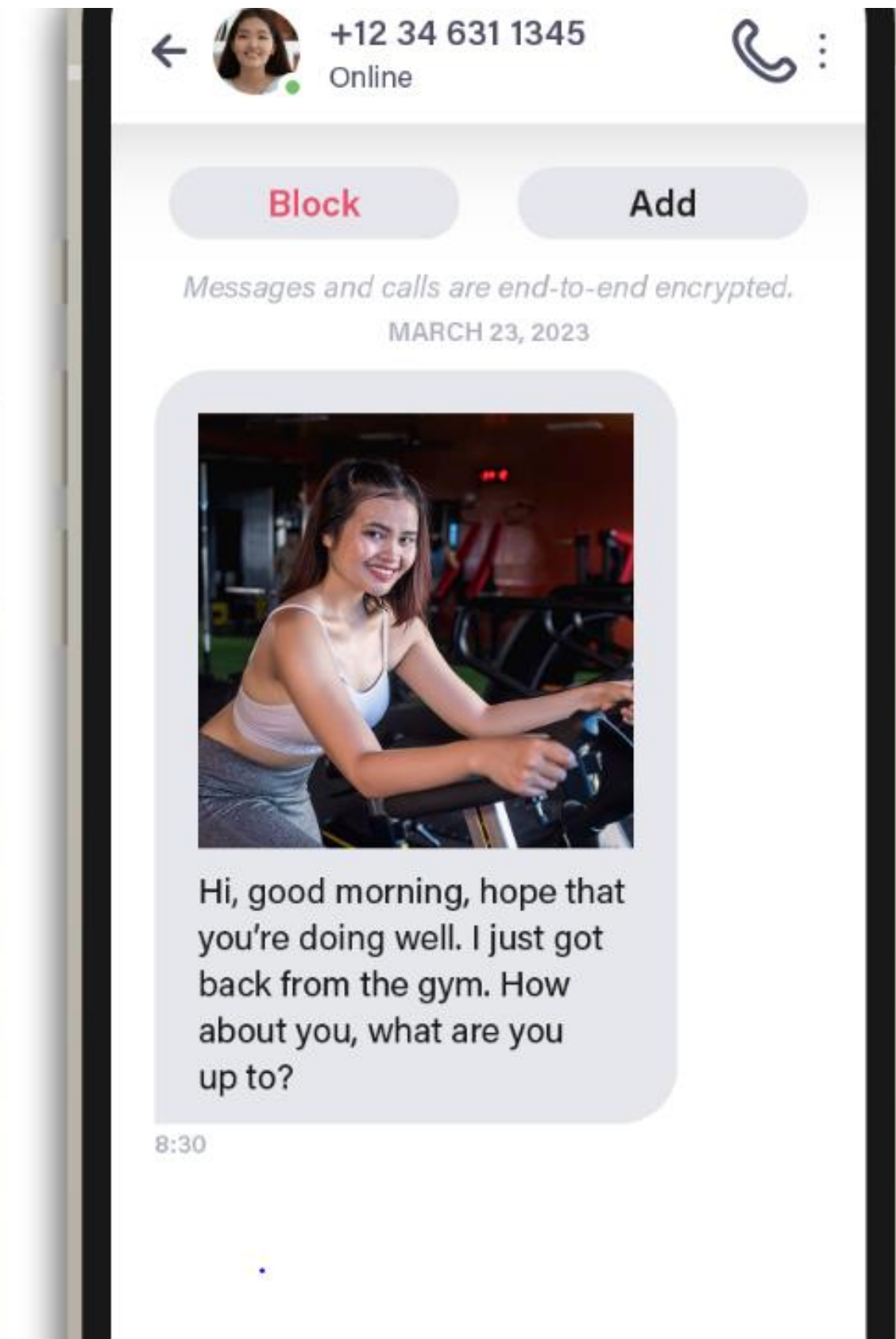
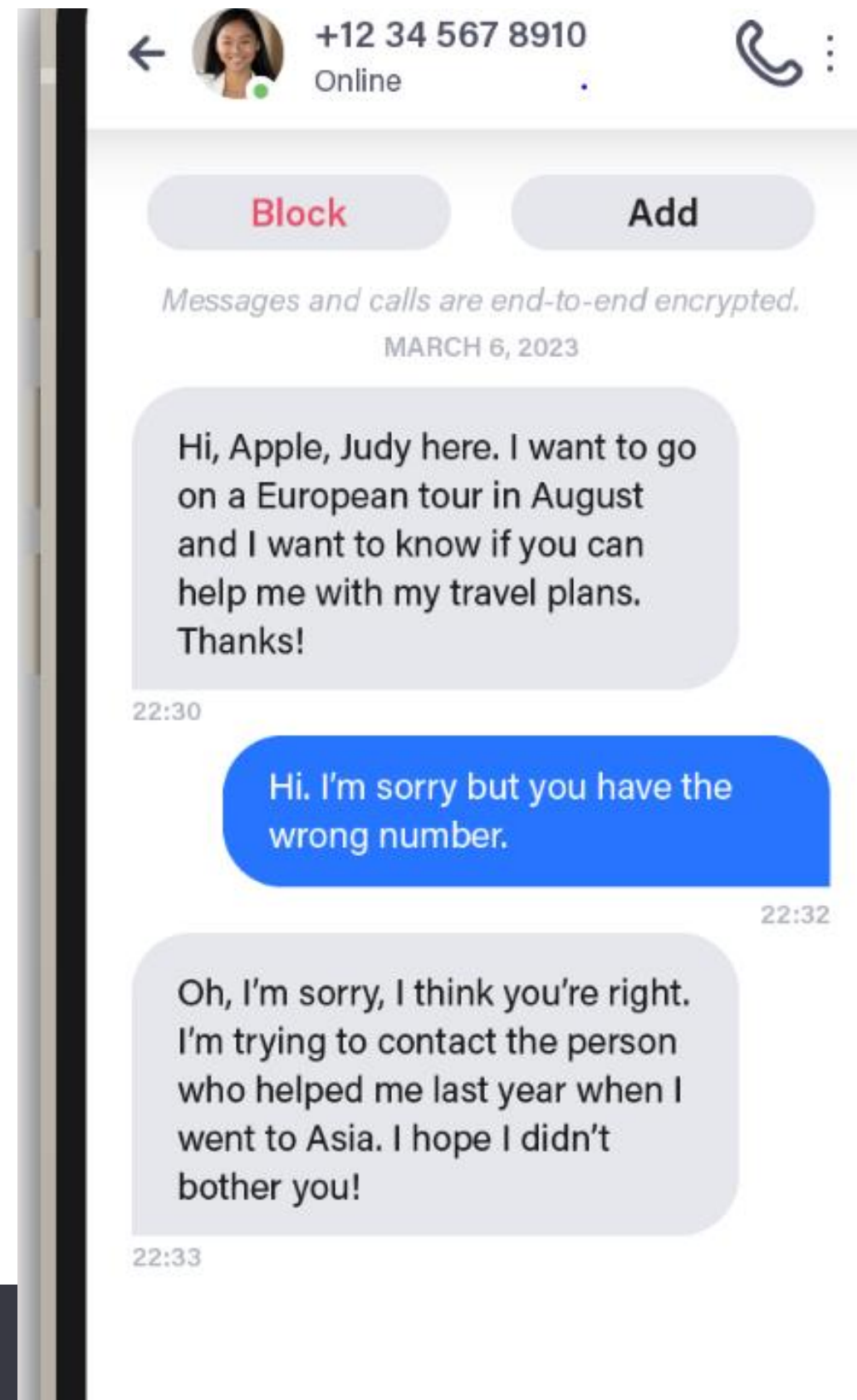
Consumer fraud (including elder fraud)

- **Synthetic identity fraud:** Combination of personally identifiable information to fabricate a fake person or entity to commit fraud
- **Romance scams:** A criminal adopts a fake online identity to gain a victim's affection and trust
- **Skimming:** When devices illegally installed on ATMs, point-of-sale (POS) terminals or fuel pumps capture data or record PINs
- **Spoofing and phishing (includes smishing and vishing):** Someone disguises an email address, sender name, phone number, or website URL to convince you that you are interacting with a trusted source



Pig Butchering

- Type of investment (cryptocurrency) fraud
- \$3.3 billion in 2022, a 127% increase
- Most targeted group is older adults (over 60), with a reported 3.1 billion loss in 2022



Pig Butchering Case - 2/24

- “Anna” – Lives on Park Ave, NYC
- Reached out to Barry May on FB
- Started chatting and sending explicit photos
- Requested crypto investment so her aunt would release her wealth
- Barry liquidated 401K and sold property – sent \$500k to invest
- FBI called before he could send more
- Left with \$10k to his name – at 62



FinCEN Alert – FIN-2023-Alert005

- Aggressive promotional campaigns and cold calls to victims
- Increased use of "money mules"
- Fraudsters use new financial products like decentralized finance (DeFi) platforms to move illicit funds and obscure their transactions
- Identified red flags that may indicate pig butchering scams
 - Sudden and high-value investments from elderly customers
 - Rapid withdrawal of funds after a large deposit
 - Frequent use of privacy coins or mixers



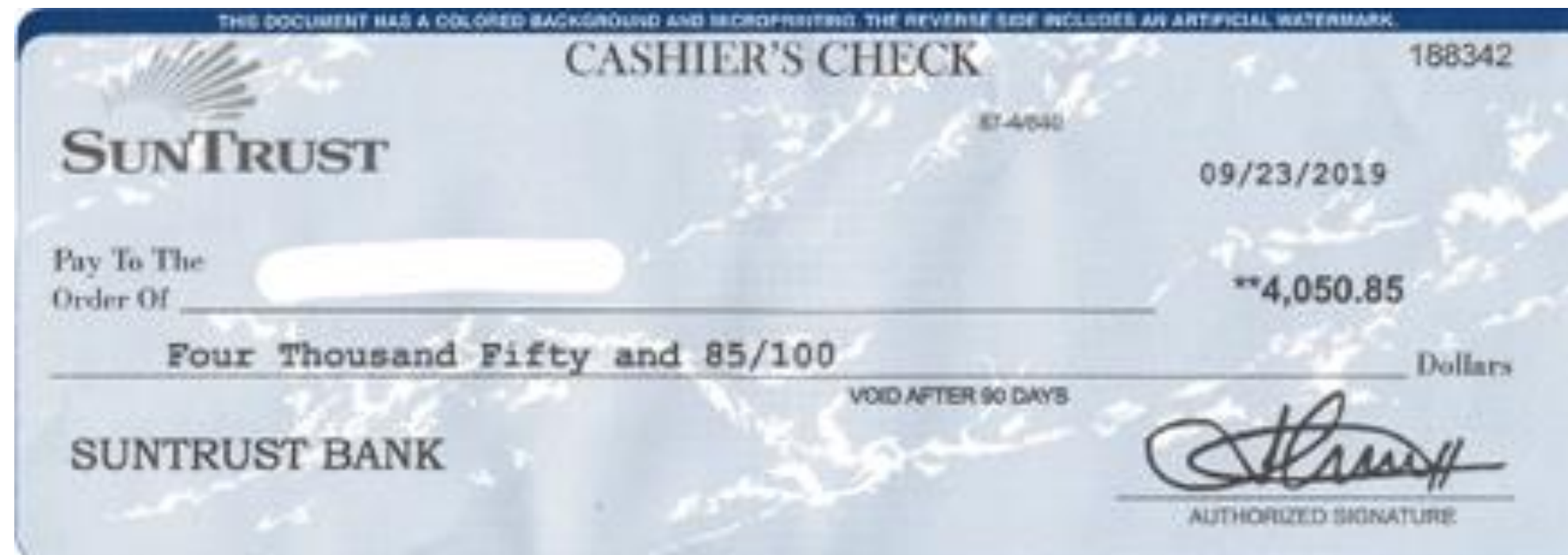
Customer education is key

- Verify the validity of any investment opportunity from strangers or long-lost contacts on social media websites
- Be on the lookout for domain names that look like legitimate financial institutions, especially cryptocurrency exchanges, but that have misspelled URLs or slight deviations in the name
- Do not download or use suspicious-looking apps as a tool for investing unless you can verify the app's legitimacy
- If an investment opportunity sounds too good to be true, it likely is - be cautious of get-rich-quick schemes



Check fraud

- \$18 billion in annual losses
- 500 million checks
- Over a million checks daily



Smaller banks are struggling to collect on bad checks from larger banks



Check fraud by mail typologies

- **Check washing:** The use of a chemical process to “wash” the ink off of a check to be replaced with a new payee and possibly a new amount
- **Photocopying:** The mass duplication of checks through sophisticated photocopying



Case Study: Regions Bank

- Operational losses related to check fraud totaled \$135 million between April and September 2023
- Regions disclosed an \$82 million loss related to check fraud in the second quarter
- Regions reported a second scheme that led to an additional \$53 million loss during the third quarter

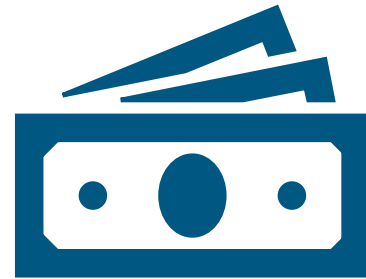


The true cost of fraud

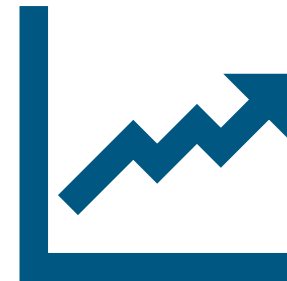
Three pillars of fraud



Overall fraud rate



Cost of technical and
human resources




Customer value impact





Economic damage


Key costs affecting banks
due to fraud are:

- Business disruption
 - Legal expenses
 - Penalties and fines
 - Customer attrition
- 

Fraud Statistics

Federal Trade Commission

2023 Statistics

 **Losses over \$10 billion to fraud**

14% increase over 2022

 **2.6 million fraud reports**

About equal to 2022

 **FIs - \$4 in costs for every dollar lost**

That's \$40 billion

 **Top methods**

Bank transfers - \$1.8 billion

Crypto - \$1.4 billion

Wires – \$343.7 million



Highest losses

- **Social media: \$1.4 billion total loss**
 - Highest overall reported loss
- **Phone calls: \$1,480 median loss**
 - Highest per person reported loss
- **Email: 358,000 reports**
 - Highest # of reports



FBI: 2023 Internet Crime Report

- 880,418 complaints (10% increase)
- Reported losses exceeding \$12.5 billion (22% increase)
 - Phishing schemes (most complaints)
 - Investment schemes (highest dollars at \$4.6 billion)
 - BEC (second highest at \$2.9 billion)
 - Victims aged 30-49 largest group
 - Victims 60 and older greatest dollars

Regulatory Risk



FinCEN Prioritizes:

- ✓ Extortion
- ✓ Social engineering
- ✓ Phishing/malware
- ✓ Business email compromise
- ✓ Ransomware



FinCEN Priorities

FinCEN Priorities - Fraud

Issued June 30, 2021 – Eight priorities to fight financial crime threats

- Fraud is believed to represent the largest share of illicit proceeds in the United States
- Proceeds from fraudulent activities may be laundered through a variety of methods, including transfers through offshore entities, accounts controlled by cyber actors, and money mules

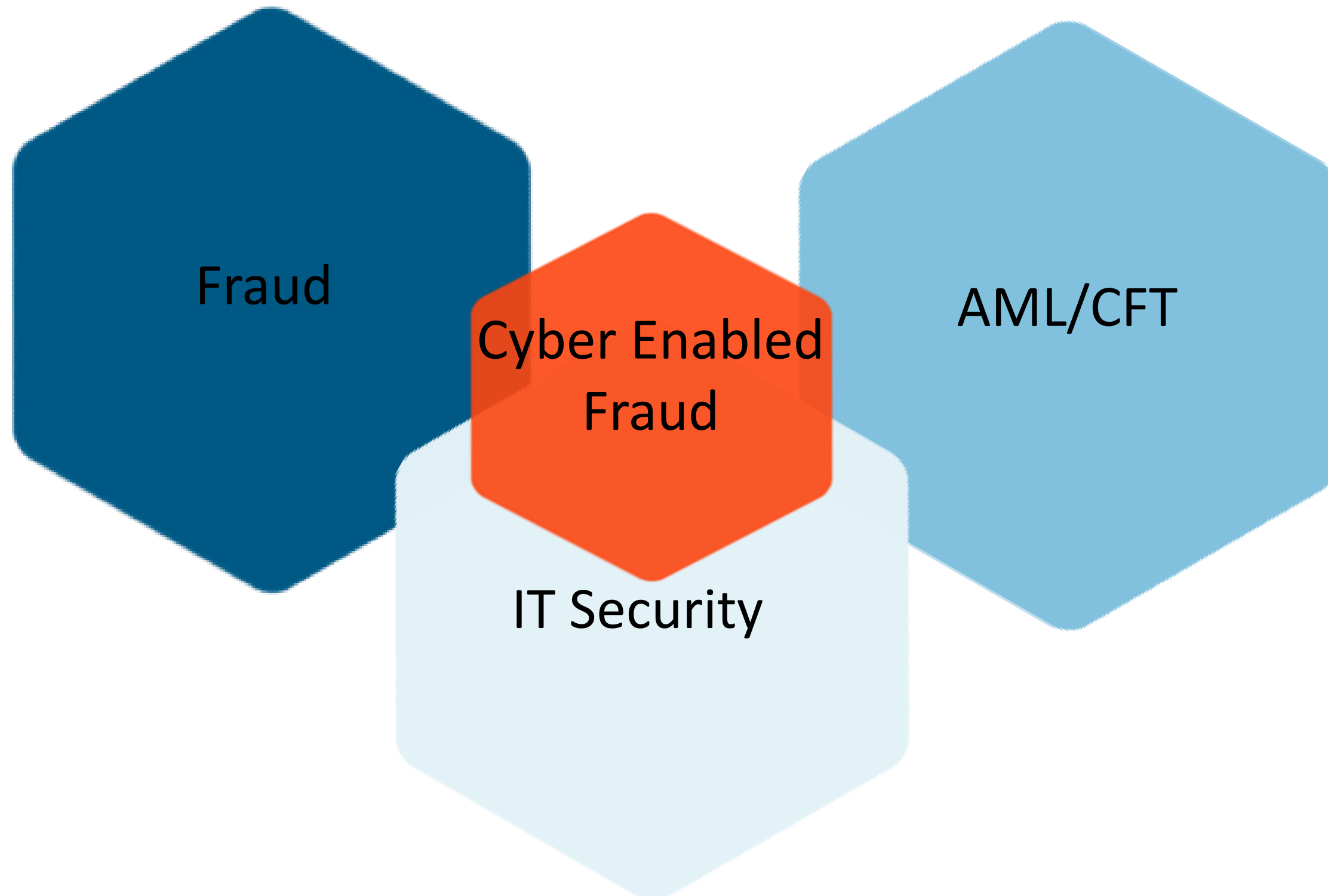
FinCEN Priorities - Cybercrime

Cybercrime is defined as any illegal activity committed via the internet or otherwise involving computer technology.

- Cybercrime is one of the most significant threats posed to financial institutions



Collaboration



Reputational Risk

The customer impact

Direct impact to bottom line if a customer falls victim to fraud

- Overall decline in customer loyalty
- Emergence of non-bank alternatives
- Identity fraud victims are 3x more likely to leave their primary financial institution
- Even when the FI is not at fault, customers are 31% more likely to leave

Media attention is not always positive



Mitigation

Fraud Risk Management

- Hardware
 - Is your business data safe?
 - Are updates and patches applied timely?
- Software
 - Fraud detection and monitoring systems
 - Check fraud
 - Wire fraud
 - ACH fraud
- People
 - Specific skill set
 - Proper training
- Dynamic processes
- Customer education



How Financial Institutions Can Help



Train financial institution staff on fraud typologies



Start or enhance a customer fraud prevention plan



Partner with local law enforcement



Connect with local organizations to educate your community

The more you know, the more you can do

- Support at the C-Suite
 - Human and technical resources are critical
- Train at onboarding
- Keep up to date with fraud reporting
 - Typologies
 - Hard dollar losses
 - Customer impact
- Ensure all stakeholders have open communication



Questions?



Thank you