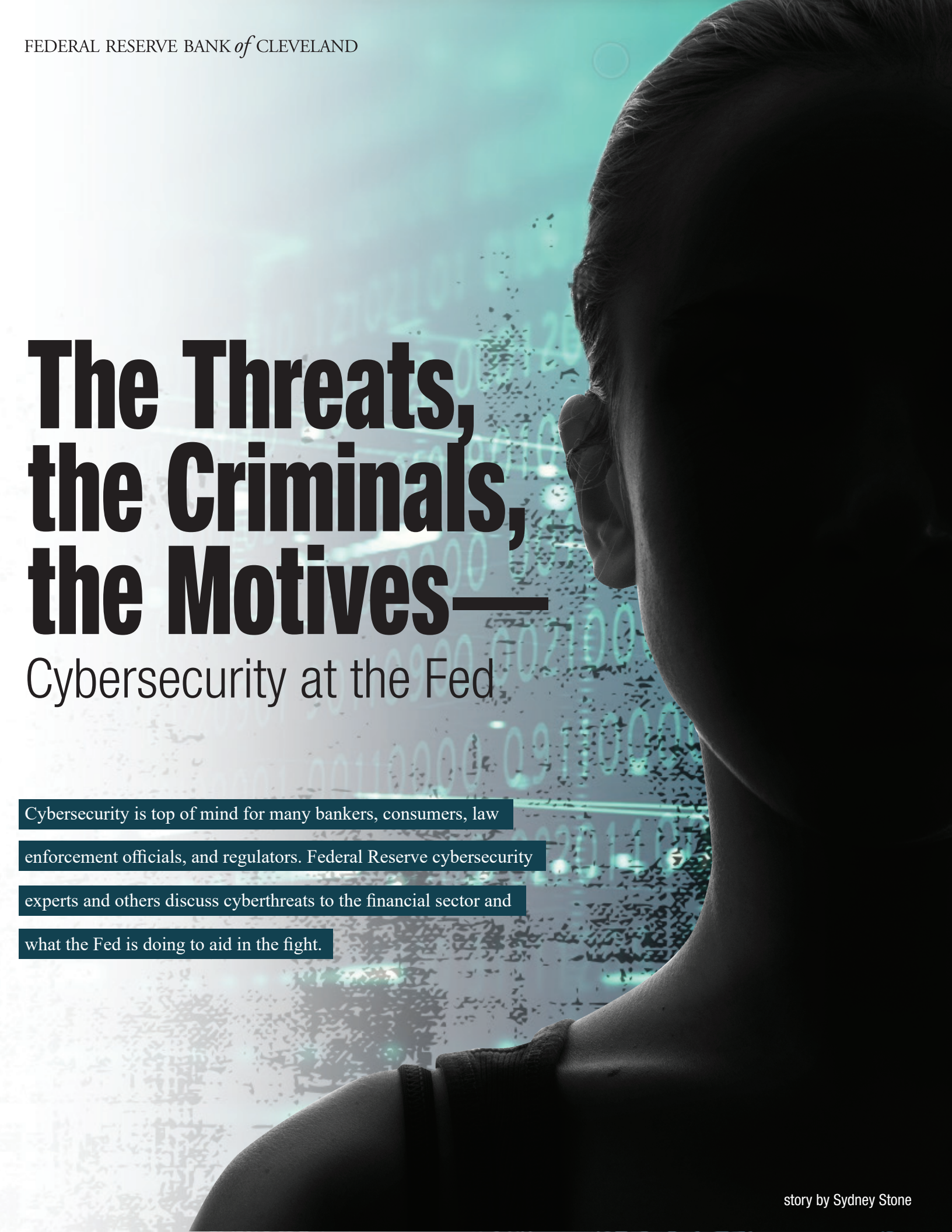
FEDERAL RESERVE BANK *of* CLEVELAND



The Threats, the Criminals, the Motives—

Cybersecurity at the Fed

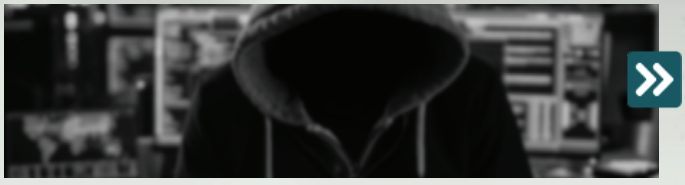
Cybersecurity is top of mind for many bankers, consumers, law enforcement officials, and regulators. Federal Reserve cybersecurity experts and others discuss cyberthreats to the financial sector and what the Fed is doing to aid in the fight.

story by Sydney Stone

Like many businesses and governments across the globe, the financial services industry is under a daily barrage of cyberattacks intended to breach data repositories, firewalls, computers, and vital information systems. The attackers' goals? To disrupt operations, conduct corporate espionage, and steal money and information. With global losses from cybertheft mounting, the pressure is on to fend off hackers, scammers, foreign intelligence agencies, and organized crime groups looking for weak spots in financial networks.

The Story

The Federal Reserve and Cybersecurity

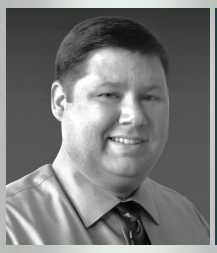


How Do Hackers Work?

Tips From the Experts: How Can Banks and Consumers Keep Information Safe?

The Experts

We interviewed two Cleveland Fed cyber experts, a Federal Reserve Board policy executive, the chief security officer of PNC Bank, and an FBI special agent. All have firsthand experience with cybersecurity in the financial sector, and their organizations often collaborate to present a united front against cybercriminals.



Jason Tarnowski
Vice president of Risk Supervision and Surveillance
Federal Reserve Bank of Cleveland

Chad Siegrist
Banking supervisor of Cyber Intelligence and Risk Management
Federal Reserve Bank of Cleveland

Deborah Guild
Chief security officer
PNC Bank, Pittsburgh, PA

Dr. Nida Davis
Associate director
Board of Governors of the Federal Reserve System, Washington DC

Ryan Macfarlane
Supervisory special agent
Federal Bureau of Investigation, Cleveland, OH

Part 1

The Federal Reserve and Cybersecurity

While individual commercial banks are responsible for their own cybersecurity, the Federal Reserve System's Supervision and Regulation Cybersecurity Analytics Support Team, or CAST, supports Fed-supervised institutions by monitoring and analyzing the threats they face. "Understanding cyberthreats against the financial sector, along with threats against other critical infrastructure components that could indirectly affect the sector, is extremely important," says Jason Tarnowski, CAST's senior officer. "It provides for more timely coordination with our financial institutions and our supervisory response."

"Understanding cyberthreats against the financial sector, along with threats against other critical infrastructure components that could indirectly affect the sector, is extremely important. It provides for more timely coordination with our financial institutions and supervisory response."

Jason Tarnowski, vice president of Risk Supervision and Surveillance, Federal Reserve Bank of Cleveland

Led by the Cleveland Fed and based in its Supervision and Regulation group, CAST assists bank supervision across all 12 Reserve Banks. The team's members have backgrounds in business and military intelligence and expertise in cyberwarfare, banking supervision, and information technology.

CAST members analyze cyber events and threats of all varieties—from high-impact cyber events that result in the loss of large amounts of sensitive data or money to low-impact threats that have little effect on financial stability or data security. Information is shared with bank examiners and others throughout the Federal Reserve System to address such events and to evaluate how threats are evolving, what new trends are emerging, and how similar attacks might unfold in the future. The goals are to increase knowledge of hacker methods and to communicate common red flags that might indicate an institution has been compromised.

CAST regularly briefs Federal Reserve System examiners on cybersecurity threats and incidents to ensure readiness and foster improved coordination of response efforts across the financial system. "CAST plays a vital role in assessing the severity of cyberattacks to the

financial sector," says Dr. Nida Davis, associate director at the Board of Governors of the Federal Reserve System. "Nobody can stop threats; what we can do is mitigate them. The nature of this work is 24/7, and we need as many qualified cyber experts on hand as possible. CAST has that expertise, which is why they are such a valuable partner in this fight."

"Nobody can stop threats; what we can do is mitigate them. The nature of this work is 24/7, and we need as many qualified cyber experts on hand as possible."

Dr. Nida Davis, associate director, Board of Governors of the Federal Reserve System

The team coordinates training exercises with regulators and banks that mimic real cybersecurity attacks and thrust participants into complex, high-pressure simulations that require quick decisionmaking.

Part of CAST's value is its ability to see the bigger picture, according to Ryan Macfarlane, a supervisory special agent for the FBI's Cleveland office who works closely with members of the team. Because the Fed's people supervise many banks and other financial organizations, they have a broader perspective of the threat landscape that means "they can often shed more light onto the level of severity of an incident," says Macfarlane. "Too often, organizations will just slap a bandage on the problem without really trying to understand the issue. This behavior opens your organization up for future vulnerability and, potentially, further loss of assets."

"They [CAST] have threat intelligence inputs, along with knowledge of the financial system infrastructure, allowing them to understand and map out the impact of an incident or active threats. Their perspective is invaluable," says Macfarlane.

CAST also understands that financial institutions need to maintain critical business functions even as they fend off hackers, says Deborah Guild, PNC Bank's chief security officer. "This frontier continues to change dynamically, and the Fed makes sure they have the right talent at the table with the knowledge to understand the balance it takes to simultaneously offer financial services and protect client data," Guild says.

"This frontier continues to change dynamically, and the Fed makes sure they have the right talent at the table with the knowledge to understand the balance it takes to simultaneously offer financial services and protect client data."

Deborah Guild, chief security officer, PNC Bank

Part 2

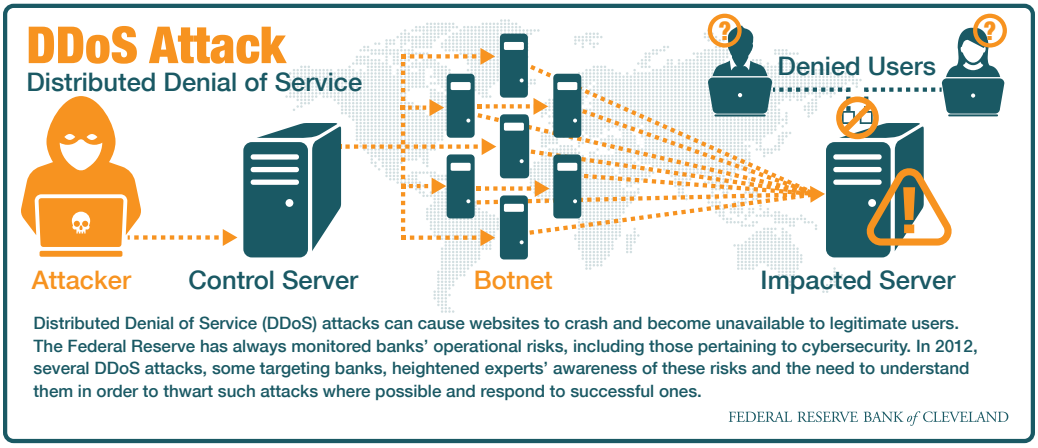
How Do Hackers Work?

The scale of attacks on financial institutions can range from a single computer or ATM to multimillion-dollar heists using global financial communications systems. Similarly, cybercriminals can be individuals operating as hacktivists or script kiddies, or they can be part of larger criminal networks or government-related nation state groups. But they all have similar motives, according to Chad Siegrist, a banking supervisor at the Cleveland Fed and the manager of CAST. "Anyway you look at it, it's greed," says Siegrist. "There's nationalistic greed, greed for power, greed for money, greed for notoriety, greed for revenge… it's pretty simple really."

"Anyway you look at it, it's greed. There's nationalistic greed, greed for power, greed for money, greed for notoriety, greed for revenge… it's pretty simple really."

Chad Siegrist, banking supervisor of Cyber Intelligence and Risk Management, Federal Reserve Bank of Cleveland

Cyberattacks take several basic forms. In the financial sector, Distributed Denial of Service (DDoS) attacks are most common. A DDoS attack uses multiple internet connections to flood and overwhelm the target and, potentially, gridlock transactions between financial institutions and their customers. The ubiquity of DDoS attacks was noted in the *Verizon 2018 Data Breach Investigations Report*, which observed that the degree of certainty of such attacks "is almost in the same class as death and taxes."



Distributed Denial of Service (DDoS) attacks can cause websites to crash and become unavailable to legitimate users. The Federal Reserve has always monitored banks' operational risks, including those pertaining to cybersecurity. In 2012, several DDoS attacks, some targeting banks, heightened experts' awareness of these risks and the need to understand them in order to thwart such attacks where possible and respond to successful ones.

FEDERAL RESERVE BANK *of* CLEVELAND

Botnets are commonly responsible for DDoS attacks. A bot is contracted when a financial institution's employees or customers accidentally download the bot, which then steals the person's credentials and uses them to log into systems and accounts.

Two attacks unique to the financial sector are payment card skimming and ATM jackpotting. These attacks are typically carried out by organized crime groups. Payment card skimming occurs when a criminal group installs a small electronic card reader into an ATM that collects data every time someone swipes a card. A member of the group has to physically return to the ATM to pick up the hardware containing the stolen data, and the information harvested allows the group to make duplicate cards or easily access bank accounts to steal money. In jackpotting, a criminal group will hack an ATM by installing software or hardware that allows it to instruct the ATM to expel thousands of dollars at a specific time on a specific day. The only thing the group needs to do is designate someone to pick up the cash.

Social attacks such as phishing and pretexting are also common against financial institutions and their customers. So are physical social engineering attacks during which cybercriminals manipulate people to obtain needed information such as answers to computer security questions. Tactics can range from impersonating the IT pro to scouring social media sites to tricking peers or colleagues to divulge information about a specific person.

"Many hackers exploit trends on social media sites that suggest that users post answers to a list of personal questions and share them with their friends and connections as a fun activity," says Davis. "These question threads are often used in social engineering attacks and are used by hackers to unlock security questions that are used to verify or breach credit card and bank accounts."

Large financial networks also have their own unique vulnerabilities. As reported in 2016, hackers stole credentials from computers of the Bangladesh central bank to gain access to the Society for Worldwide Interbank Financial Telecommunications (SWIFT) system, a network with thousands of member institutions. The thieves were able to craft and send authenticated SWIFT messages directing the New York Fed to transfer $81 million from the Bangladesh account to accounts in the Philippines and Sri Lanka. A North Korean man working for the North Korean government-sponsored "Lazarus Group" was charged with conspiracy in the Bangladesh SWIFT attack in a complaint filed in US federal court in June.

The Bangladesh central bank attack is just one instance in a string of many multimillion-dollar thefts from banks in Russia, Ecuador, and Taiwan using fraudulent orders sent via SWIFT. "The point of the internet is to connect us all. If you have the right motivation, the right tech, and the right targets, you can have worldwide impact," says Macfarlane.

"The point of the internet is to connect us all. If you have the right motivation, the right tech, and the right targets, you can have worldwide impact."

Ryan Macfarlane, supervisory special agent, Federal Bureau of Investigation

Part 3

Tips From the Experts: How Can Banks and Consumers Keep Information Safe?

Protecting against cyber intrusions starts with communication. "For financial institutions, it's imperative that they work to cultivate a culture of cyberawareness among employees and practice good cyberhygiene," Davis says. "Cybersecurity is not just an IT problem; it is everyone's problem." For example, properly patching and updating networks, encrypting data, frequent and accurate security scanning, using password vaults, requiring two-factor authentication on accounts when possible, and training employees on how to exercise vigilance against cybercriminals are all practices advocated by cybersecurity experts. Number one among these practices is training people to safeguard against social engineering. No matter how good your antivirus software or firewalls are, it's hard to predict how a cybercriminal might hack one of your human assets.

Protect Your Assets on the Internet: Best Practices from the Pros

Consumers

- Put the highest possible privacy/security setting on your social media accounts
- Use two-factor authentication on bank and credit card accounts
- Freeze your credit—this will put a protection in place if your identity is stolen
- "Harden" your systems by updating software

Financial Institutions and Businesses

- Educate employees to guard against social engineering attacks—especially those attempted through email
- Properly encrypt important data and information
- Use password vaults to store passwords shared by groups of people
- Understand what devices are connected to each other and how to manage their security

FEDERAL RESERVE BANK *of* CLEVELAND

Consumers and other end users need to keep up with software updates. Tailoring social media accounts to have the most stringent security possible is also a must. So is cultivating a healthy suspicion of email attachments and social media direct messages. Guild suggests a credit freeze and establishing separate passwords for accessing a joint bank or credit card account if you hold

one with a spouse or significant other. Siegrist emphasizes the importance of long passwords; they do not need to be complicated, but they should be difficult to guess (for example, Mycoffeeisblackbutmyhouseisred07), because it takes password hacking technology years to hack into lengthy passwords.

In addition to practicing good cyberhygiene and protecting personal information, it also helps to simply pay attention—especially in large crowds. Cybercrime activity can increase during events that draw large crowds of people who may be distracted or in a rush and thus less likely to safeguard credit cards and financial information. In Cleveland, Ohio, the 2016 World Series brought spikes in computer-related fraud, according to Macfarlane. Large, globally attended events such as the Olympics also see upticks in cybercrime.

"I can't tell you what the next threat is, but it will materialize. Practicing constant vigilance is key."

Jason Tarnowski, vice president of Risk Supervision and Surveillance, Federal Reserve Bank of Cleveland

The simple truth, though, is that there is never a guarantee of complete cybersecurity, even with up-to-date software, carefully chosen passwords, and adherence to other sound protocols. But those practices do help shrink and manage unrelenting risk, according to the Cleveland Fed's Tarnowski. "I can't tell you what the next threat is, but it will materialize," Tarnowski says. "Practicing constant vigilance is key."

Related Content

- Explore a Federal Reserve payments fraud study
  - https://tinyurl.com/pymtfraudfrb
- Learn how to recover from identity theft with some tips from the Federal Trade Commission
  - https://tinyurl.com/itftctips
- Read about how to be vigilant against cyberfraud
  - https://tinyurl.com/cyberfraudfrbc