Treasury Management Best Practices

AASBO Conference

May 6, 2021

Jennifer B. Luster, CTP
Regions Bank Treasury Management Relationship Manager

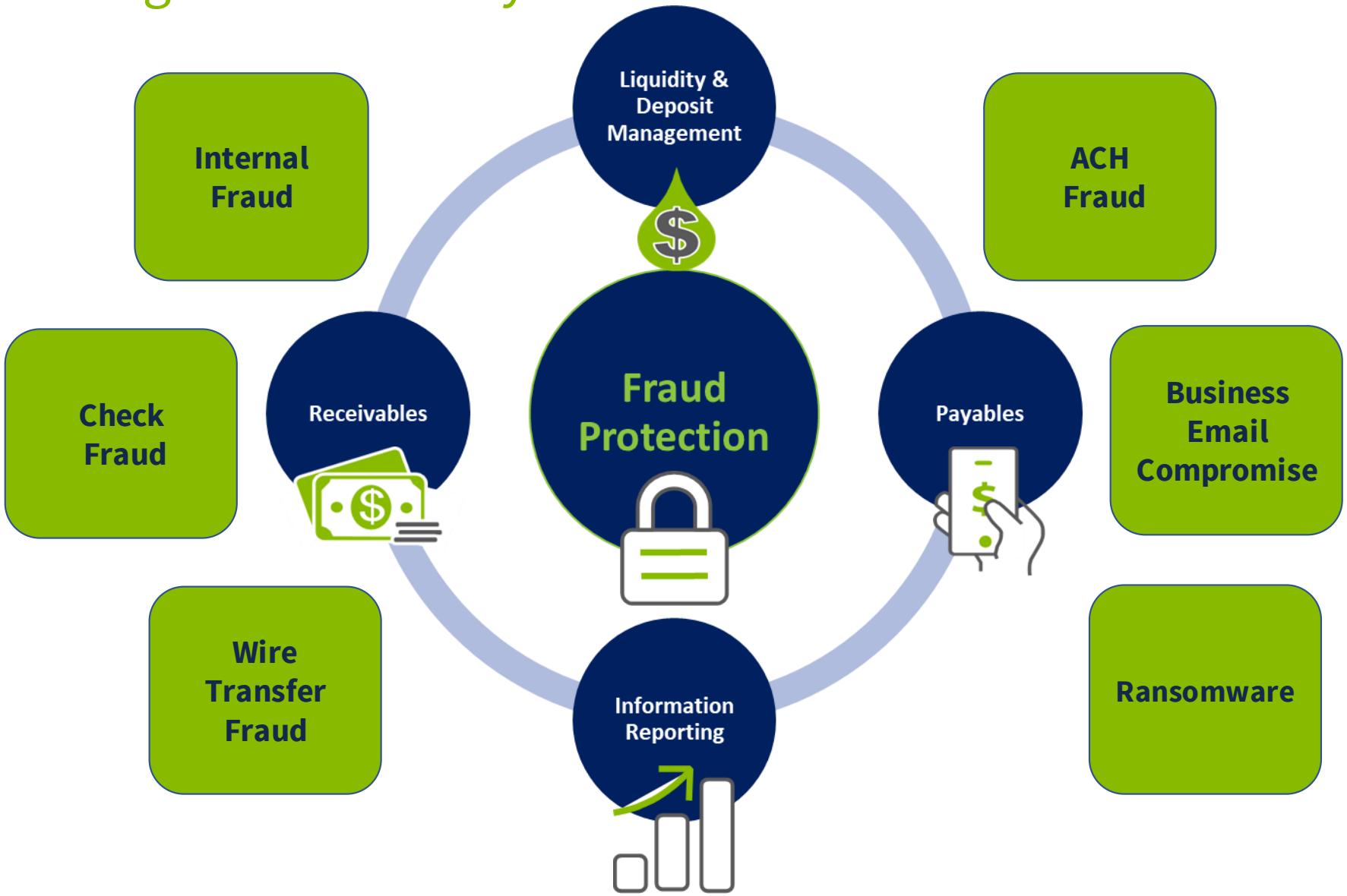
Contina Woods, CTP
Regions Bank Treasury Management Relationship Manager

REGIONS

Agenda

- Introductions
- Treasury Management & Types of Payment Fraud
- AFP Payment Fraud Highlights
- Business Email Compromise
- Ransomware
- Best Practices
- Incident Response Plan
- Fraud Recovery
- Questions

Treasury Management and Payment Fraud



Payment Fraud and Control Survey Highlights

- Nearly 75% of organizations were targets of a payment fraud attack in 2020.
- 65% of survey respondents believe some share of the increase in fraud was due to the pandemic.
- Checks and wire transfers remain the payment methods most impacted by fraud activity.
- Check fraud in 2020 was at its lowest level since 2008 which is a result of organizations using fewer checks in their business-to-business transactions.
- Wire fraud continues to be high although it is on a downward trend suggesting companies are more efficient at identifying fraud quickly and using processes to minimize fraud risk.
- ACH debit fraud has increased indicating perpetrators are targeting ACH payment methods more frequently than check and wire transfers.
- Corporate and commercial credit card fraud decreased substantially in 2020.
- Business email compromise was the primary source of payment fraud attacks in 2019 and 2020.

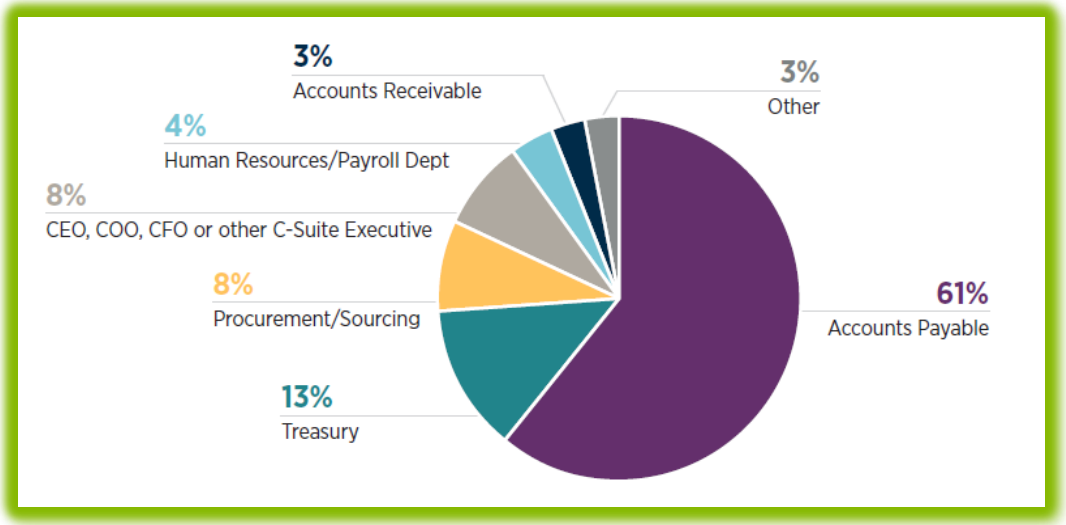
2021 AFP® Payments Fraud and Control Survey Report: Highlights | www.AFPonline.org
*The report was produced using 534 survey responses from corporate practitioners.

Payment Fraud and Control Survey Highlights

Percent of Organizations that Experienced Attempted and/or Actual Payments Fraud, 2010-2020

Percent of Organizations that Experienced Business Email Compromise (BEC), 2015-2020

Departments Most Vulnerable to Being Targeted by BEC Fraud (Percentage Distribution of Organizations)



2021 AFP® Payments Fraud and Control Survey Report: Highlights | www.AFPonline.org

Business Email Compromise

- Targets employees with access to company finances
- Directs employee to release funds to bank accounts thought to belong to trusted partners

Iterations Over Time:

- **Executive email intrusion:** criminal impersonates senior executive requesting payment or order to purchase gift cards
- **Vendor email intrusion:** criminal impersonates vendor requesting the company to change payment remittance information
- **Employee email intrusion:** criminal impersonates an employee requesting the vendor to send payment account information or requesting the company change employee's direct deposit information

Most Prevalent Types of BEC Fraud (Percent of Organizations)

	LESS THAN 25 INSTANCES ANNUALLY	26-100 INSTANCES ANNUALLY	101-200 INSTANCES ANNUALLY	200+ INSTANCES ANNUALLY
Emails from other third parties requesting changes of bank accounts, payments instructions, etc.	88%	9%	2%	1%
Emails from fraudsters pretending to be senior executives using spoofed email domains directing finance personnel to transfer funds to fraudsters' accounts	87%	9%	2%	2%
Emails from fraudsters impersonating as vendors (using vendors' actual but hacked emails addresses) directing transfers based on real invoices to the fraudsters accounts	87%	11%	1%	1%

2021 AFP® Payments Fraud and Control Survey Report: Highlights | www.AFPonline.org

Ransomware

- Fraudsters target an organization by placing malware on the organization's computer system and locking the system with encryption.
- Payment (ransom) is demanded before the fraudster releases the code to unlock the system.
- Fraudsters access the computer system through:
  - Infected software applications
  - Infected documents and files
  - Infected external storage devices
  - Compromised websites

Examples or ransomware in the public sector

- A U.S. county was infected by Ryuk, taking almost all of the county's systems offline. The county had backup servers, but they were not isolated from the network, allowing them to be infected as well. The county paid a $132,000 ransom.

- A U.S. city's systems were infected by Robbinhood with a ransom demand of 13 Bitcoins ($76,000). The attackers entered the network through old, out-of-date hardware and software. The ransom was not paid, but service restoration was estimated to cost over $9 million.

https://www.cisa.gov/sites/default/files/2021-01/NCIJTF%20Ransomware_Fact_Sheet.pdf

Ransomware

The Threat and How It Impacts Remote Learning Education

The Cybersecurity and Infrastructure Security Agency (CISA) has seen an increase in malicious activity with ransomware attacks against K-12 educational institutions. Malicious cyber actors are targeting school computer systems, slowing access, and rendering the systems inaccessible to basic functions, including remote learning. In some instances, ransomware actors stole and threatened to leak confidential student data unless institutions paid a ransom.

Since March, uninvited users have disrupted live-conferenced classroom settings by verbally harassing students, displaying pornography and violent images, and doxing meeting attendees.

For detailed information on these threats and actions to take, visit the Joint Cybersecurity Advisory on this topic, jointly developed by CISA, FBI, and the Multi-State Information Sharing and Analysis Center.

https://www.cisa.gov/sites/default/files/publications/Cyber_Threats_to_K-12_Remote_Learning_Fact_Sheet_15_Dec_508.pdf

Cyber Security Best Practices

To minimize service disruptions, CISA encourages educational providers to review and establish patching plans, security policies, user agreements, and business continuity plans to ensure they address current threats posed by cyber threat actors.

PREPARING FOR LIKELY ATTACKS

- Patch operating systems, software, and firmware as soon as manufacturers release updates.
- Regularly change passwords to network systems and accounts, and avoid reusing passwords for different accounts.
- Use multi-factor authentication where possible.
- Set antivirus and anti-malware solutions to automatically update and conduct regular scans.
- Monitor privacy settings and information available on social networking sites.
- Do not pay ransoms. Payment does not guarantee files will be recovered. It may also inspire cyber actors to target additional organizations, encourage other criminal actors to engage in the distribution of ransomware, and fund illicit activities.
- Configure network firewalls to block unauthorized IP addresses and disable port forwarding.

https://www.cisa.gov/sites/default/files/publications/Cyber_Threats_to_K-12_Remote_Learning_Fact_Sheet_15_Dec_508.pdf

Cyber Security Best Practices

- *Ensure* participants use the most updated version of remote access/meeting applications. Require passwords for session access.
- *Encourage* students to avoid sharing passwords or meeting codes.
- *Establish* a vetting process to identify participants as they arrive, such as a waiting room.
- *Establish* policies to require participants to sign in using true names rather than aliases. Ensure only the host controls screensharing privileges.
- *Implement* a policy to prevent participants from entering rooms prior to host arrival and to prevent the host from exiting prior to the departure of all participants.

https://www.cisa.gov/sites/default/files/publications/Cyber_Threats_to_K-12_Remote_Learning_Fact_Sheet_15_Dec_508.pdf

Fraud Prevention Best Practices

- Utilize dual controls, online user entitlements, separation of duties and audit processes
- Reconcile accounts daily and utilize check fraud/electronic debit fraud prevention services
- Decrease check volume by converting payments to card or ACH
- Utilize a dedicated PC protected with Anti-Virus/Anti-Malware software for cash management functions
- Create strong passwords and change them often
- Do not click on links or attachments in emails from an unknown source
- Store check stock, deposit slips and bank statements in a secured location
- Place stop payments / positive pay voids on stale dated outstanding checks
- Call an authorized contact to verify any transfer of funds or change in remittance information using a phone number from the company records
- Use MCC blocks, dollar limits and administrator safeguards on card programs
- Educate your employees on fraud risks and prevention

The Cybersecurity & Infrastructure Security Agency

The Cybersecurity & Infrastructure Security Agency (**www.cisa.gov**), a division of the Department of Homeland Security, has created a comprehensive guide to assist businesses in creating the foundation of such a plan.
The Agency suggests four steps to consider in preparing for a potential attack:

CONNECT: Reach out and develop relationships in your community, including with local law enforcement. Having these relationships established before an incident occurs can help speed up the response when something happens.

PLAN: Take the time now to plan on how you will handle a security event should one occur. Learn from previous events or the experiences of others to inform your plans.

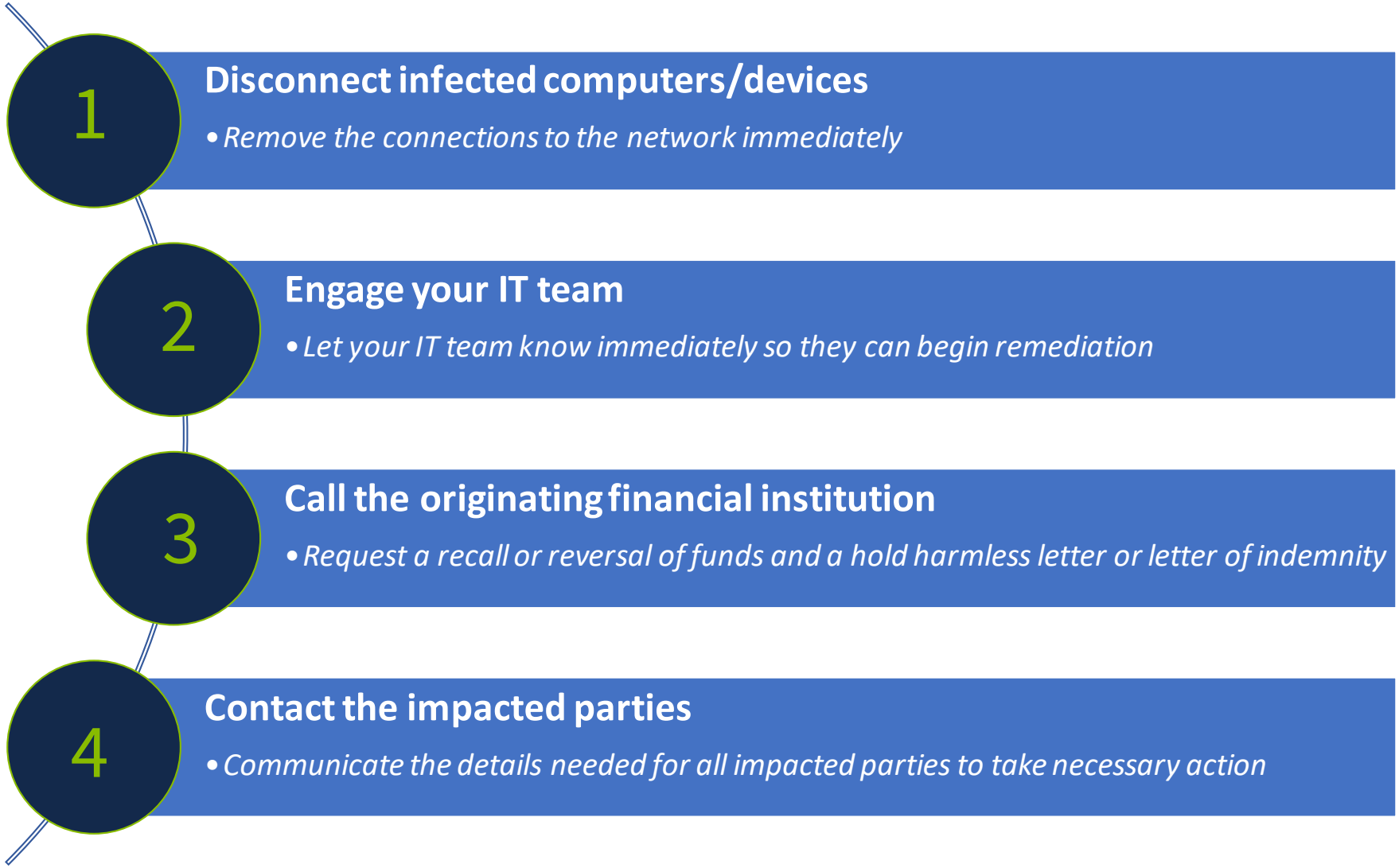
TRAIN: Provide your employees with training resources and exercise your plans often. The best laid plans must be exercised in order to be effective.

REPORT: Call local law enforcement if you encounter anything suspicious.

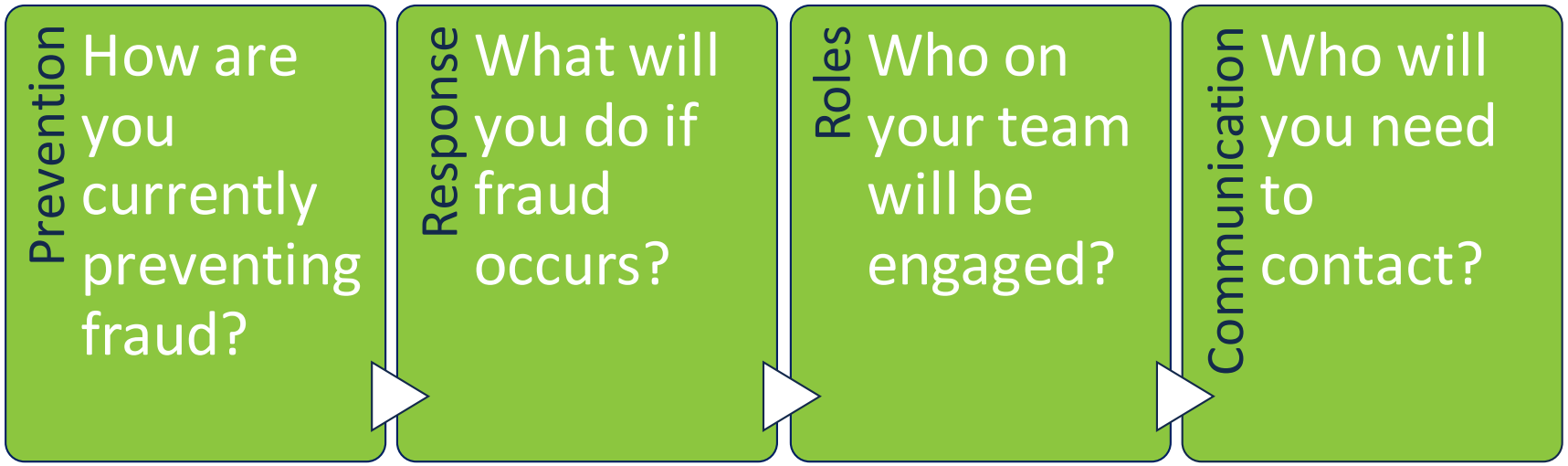
Developing your Incident Response Plan will provide a guide to follow in the event of an attack. The best time to develop a relationship with law enforcement and corporate partners who will assist in a cyber event is not during or after the event. Relationships with federal law enforcement partners like the FBI, DHS and Secret Service should be cultivated in the present with ongoing dialog and sharing of best practices. Create a plan to protect your business and your employees from fraud threats.

You can find more information on preparing your plan at *cisa.gov/publication/connect-plan-train-report*.

When fraud occurs, what are the next steps?



Prevention and Recovery – Are you prepared?



A response and recovery plan will allow you to act FAST if fraud occurs to minimize damage and loss.

Questions?

Disclaimer:
The opinions expressed in the presentation are statements of the speaker's opinion, are intended only for informational purposes, and are not formal opinions of, nor binding on Regions Bank, its parent company, Regions Financial Corporation and their subsidiaries, and any representation to the contrary is expressly disclaimed**.**

The information presented is general in nature. Presentation material sourced from the Association for Financial Professionals, and the Department of Homeland Security are noted. Regions reminds its customers to be vigilant about fraud and security, and they are responsible for taking action to protect their computer systems. Fraud prevention requires a continuous review of your policies and practices, as the threat evolves daily. There is no guarantee all fraudulent transactions will be prevented or that relatedfinancial losses will not occur.