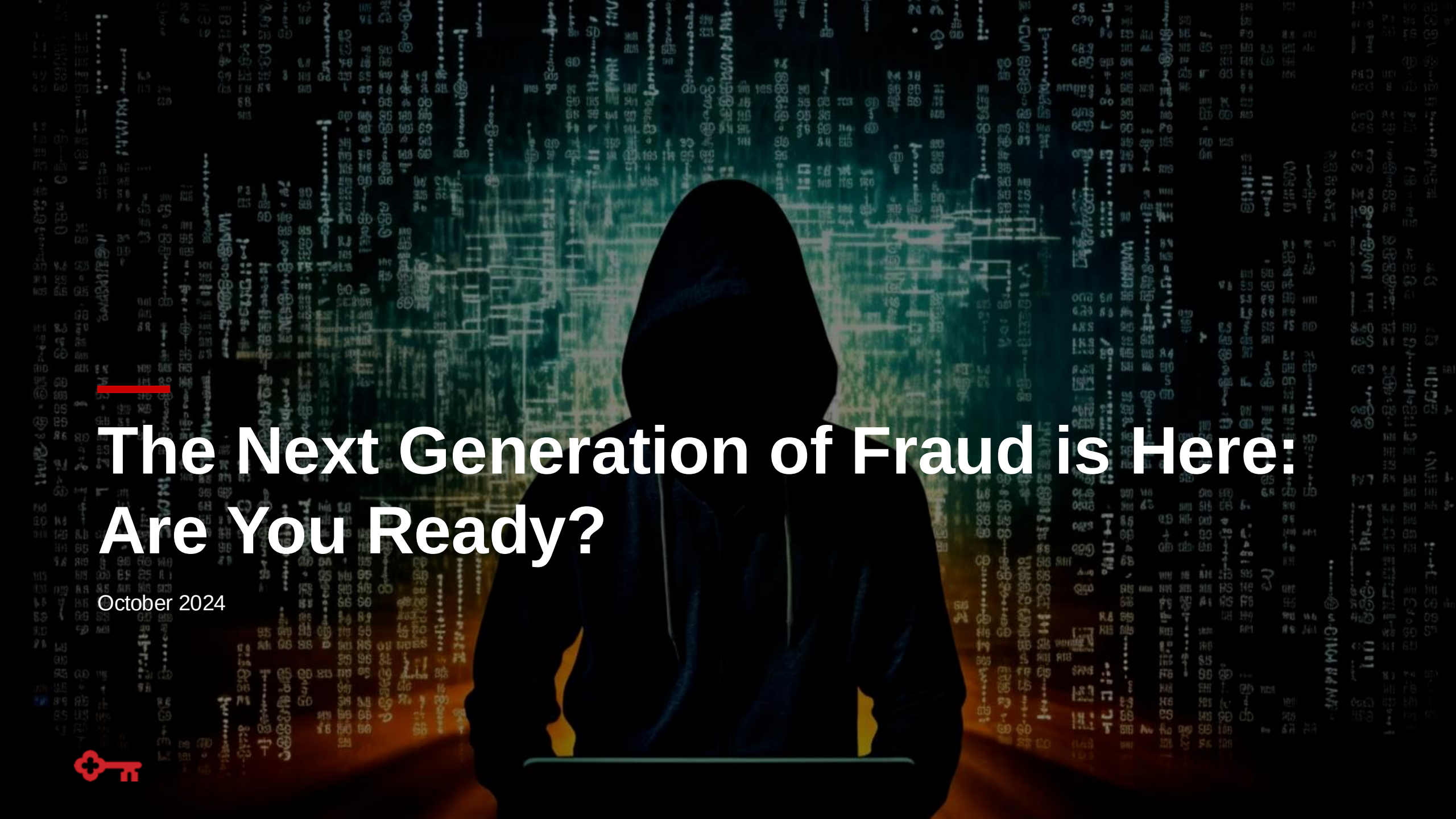
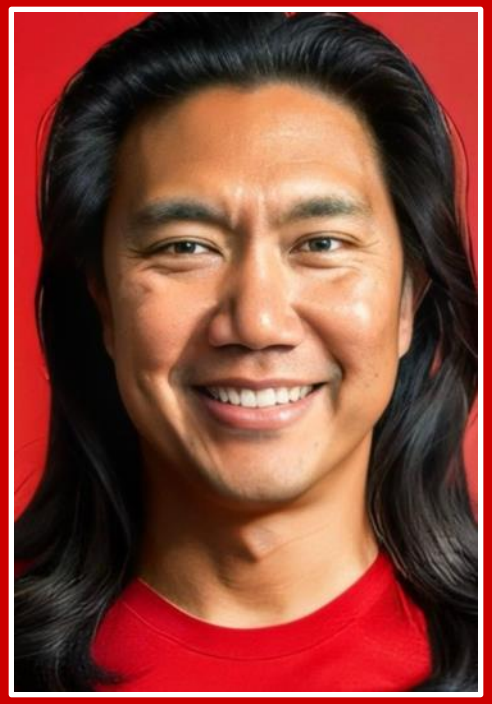


# The Next Generation of Fraud is Here: Are You Ready?

October 2024

# Today's Speakers



**Miguel Navarro**
Head of Client Verification & Authentication
KeyBank

**Jillian Burner**
Cybersecurity Advisor
Cybersecurity and Infrastructure Security Agency (CISA)

**Michael Gerfin**
Supervisory Special Agent
FBI, Cleveland Division

# Agenda

- The Evolving Cyber and Fraud Landscape
- Next-Gen Fraud Tactics
- Defensive Strategies Against Sophisticated Attacks
- KeyBank’s Commitment to Fraud Prevention
- Q&A

# Increasing sophistication in cyber and fraud tactics

**Advanced Techniques**

Cybercriminals are employing more sophisticated methods, such as AI-driven attacks and deepfakes, to bypass traditional security measures.

**Coordination and Collaboration**

Fraudsters often operate in organized groups, coordinating attacks to exploit system vulnerabilities more effectively.

**Evolving Strategies**

Cybercriminals continuously adapt to new technologies and countermeasures, making it harder for static defenses to keep up.

# The Evolving Cyber and Fraud Landscape

## Current Trends

**20%**

of respondents identified increasingly sophisticated fraud tactics as the leading cause of attempted fraud.

**75%**

of banks, fintechs, and credit unions are planning to invest in an identity risk solution to combat fraud.

**62%**

of surveyed banks said fraud most commonly occurs on mobile and online/digital services.

Source: 2024 State of Fraud Benchmark Report | Alloy

# The Evolving Cyber and Fraud Landscape

## Emerging Threats

### Artificial Intelligence

How fraudsters use AI to enhance cyberattacks

### Deepfakes

How fraudsters power distrust and misinformation

### Mobile Device Hacking

The vulnerability of smartphones

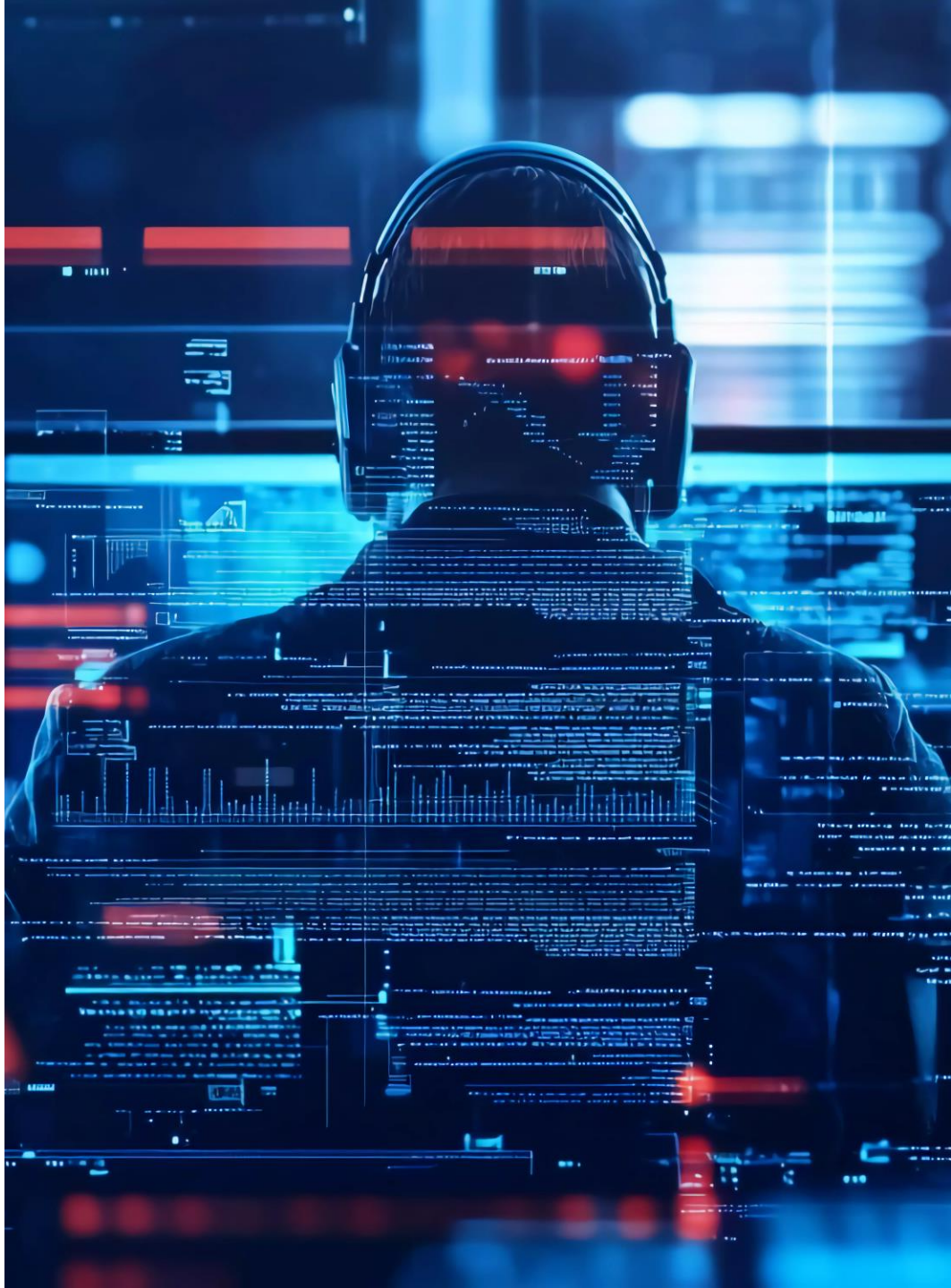

Deep Dive
Next-Gen Fraud Tactics

# Next-Gen Fraud Tactics

## Artificial Intelligence

### AI cybersecurity and fraud threats

- **Automated attacks:** AI can be used to automate, and scale cyberattacks, making them more efficient and harder to detect.
- **Advanced social engineering:** AI can generate highly personalized phishing attempts by analyzing large datasets on potential targets.
- **Vulnerability discovery:** AI systems can be used to rapidly identify software vulnerabilities for exploitation.
- **Evasion of security systems:** AI can help malware evolve to avoid detection by traditional security measures.



# Next-Gen Fraud Tactics

## AI and deepfakes

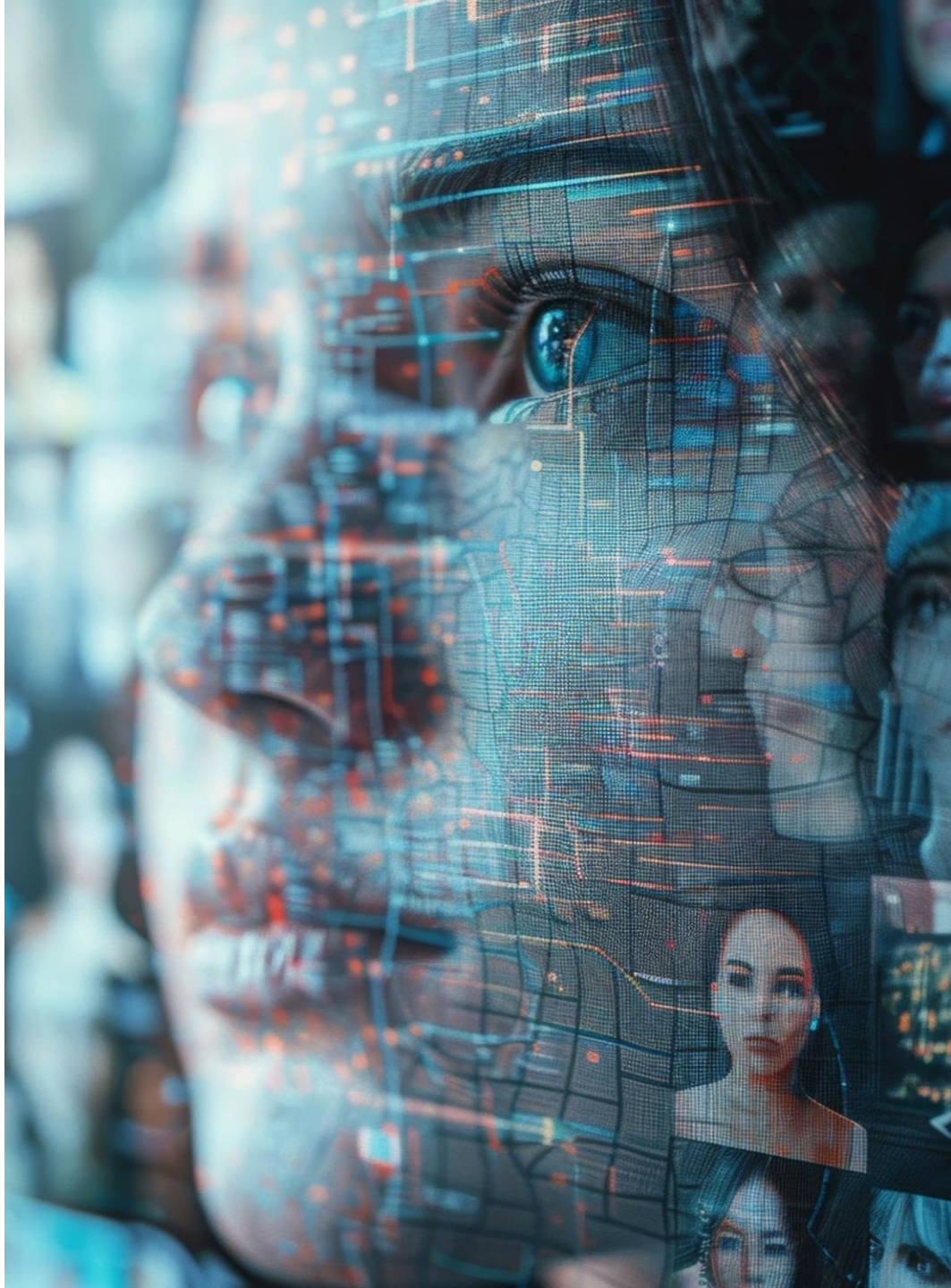
### Deepfakes and their role in social engineering

- **Roles:** Impersonation, phishing, fraud, disinformation, blackmail
- **Impacts:** Mistrust
- **Prevention:** Detection, awareness, verification

*“The tools and techniques for manipulating authentic multimedia are not new, but the ease and scale with which cyber actors are using these techniques are. …. Organizations and their employees need to learn to recognize deepfake tradecraft and techniques and have a plan in place to respond and minimize impact if they come under attack.”*

- Candice Rockell Gerstner, NSA Applied Research Mathematician who specializes in Multimedia Forensics[1]

1. NSA, U.S. Federal Agencies Advise on Deepfake Threats, September 2023



# Next-Gen Fraud Tactics

## Mobile Device Hacking

### Methods hackers use to compromise mobile devices

1. **Malware**
2. **Phishing**
3. **Man-in-the-Middle Attacks**
4. **Exploiting Vulnerabilities**
5. **Social Engineering**
6. **SIM Swapping**

**80%** of phishing phishing sites now target mobile devices, and users are 6–10 times more likely to fall for SMS phishing attacks.

**67%** of remote workers admitted to failing to fully adhere to corporate cybersecurity policies.



1. Zimperium, 2023 Global Mobile Threat Report
2. Posey, C., and Shoss, M. Research: Why Employees Violate Cybersecurity Policies. Retrieved from https://par.nsf.gov/biblio/10490055. Harvard Business Review


Defensive Strategies
Are You Ready?

# Defensive Strategies

## New Technology and Training

Importance of staying ahead with **cutting-edge security technologies**

AI and Machine Learning

Blockchain Technology

Advanced Encryption

**Continuous education and training** for employees

Regular Training Programs

Simulated Attacks

Security Awareness Campaigns

# Defensive Strategies

## Multi-Factor Authentication (MFA)

Benefits of MFA and other robust authentication methods

### Enhanced Security

MFA significantly reduces the risk of unauthorized access

### User Confidence

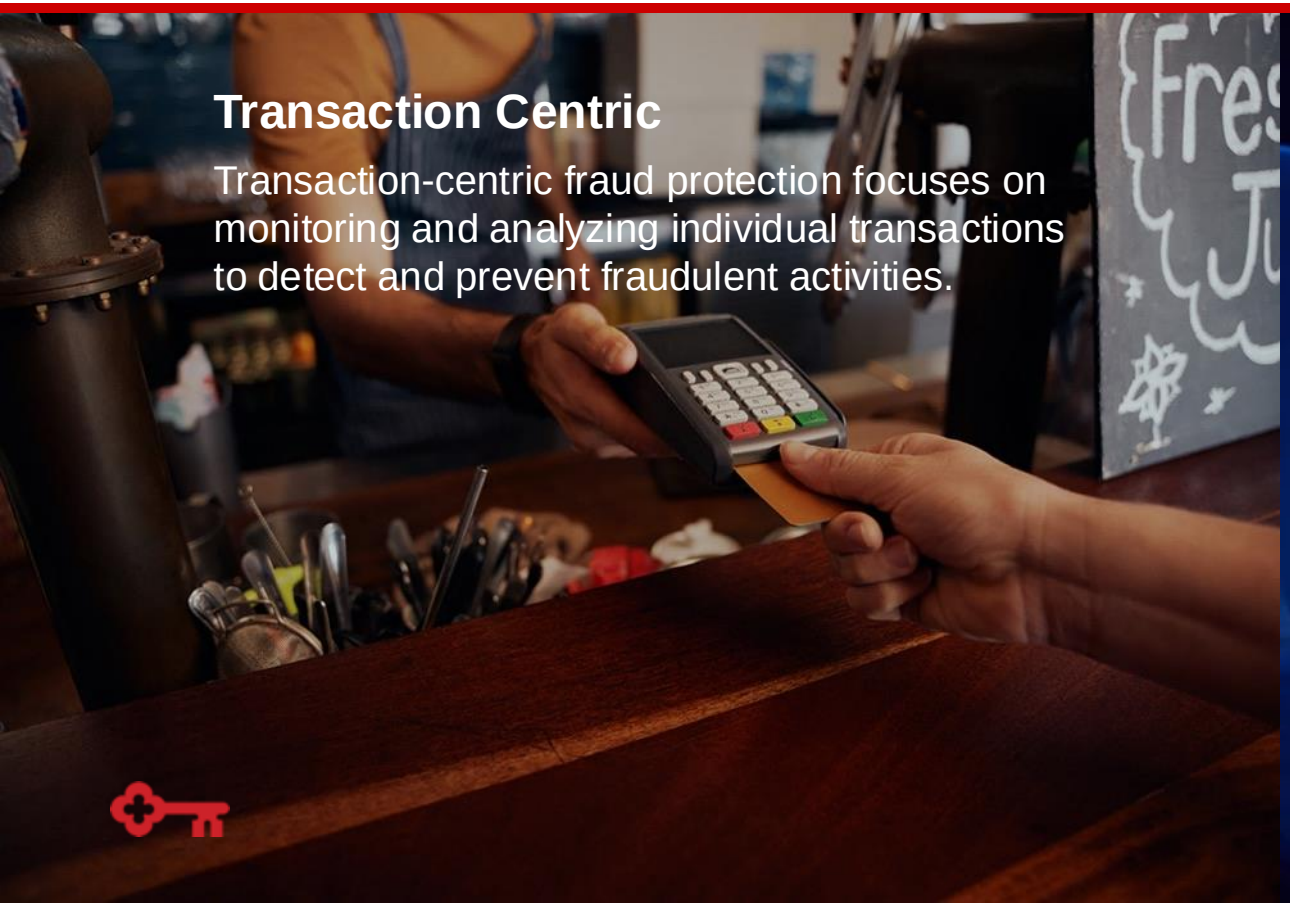
Increases user confidence in the security of accounts

### Reduced Fraud

Drastically lowers the incidence of account takeovers

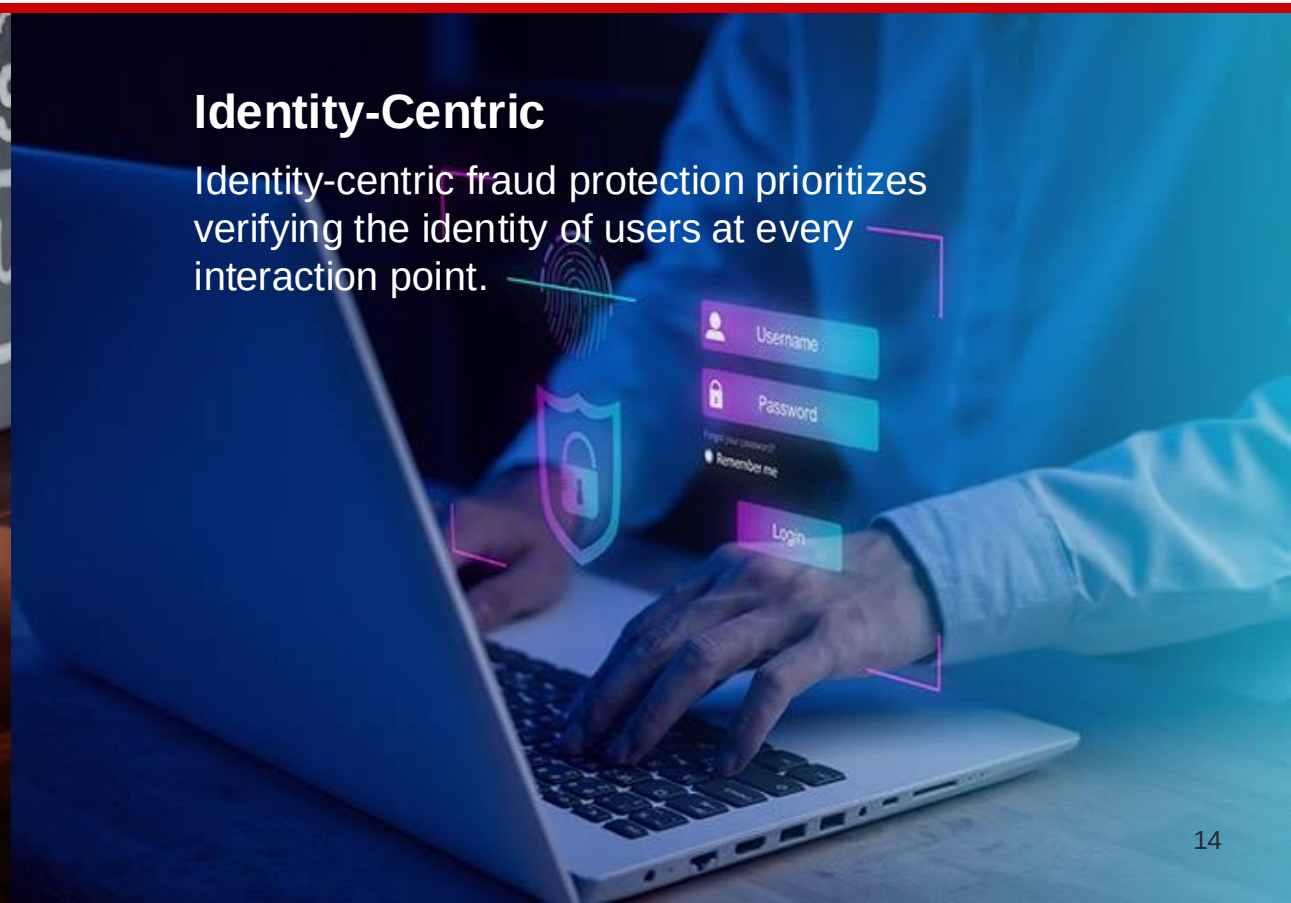
# Defensive Strategies

## Identity-Centric Fraud Models



### Transaction Centric

Transaction-centric fraud protection focuses on monitoring and analyzing individual transactions to detect and prevent fraudulent activities.




### Identity-Centric

Identity-centric fraud protection prioritizes verifying the identity of users at every interaction point.

# Defensive Strategies

## Identity-Centric Fraud Models

Benefits

**Enhanced Fraud Detection**

More effective at detecting sophisticated fraud

**Improved User Experience**

Reduces friction for legitimate users

**Scalability**

Easily scalable to handle growing user bases

# KeyBank's Commitment to Fraud Prevention

# Education:
## What is KeyBank Doing?

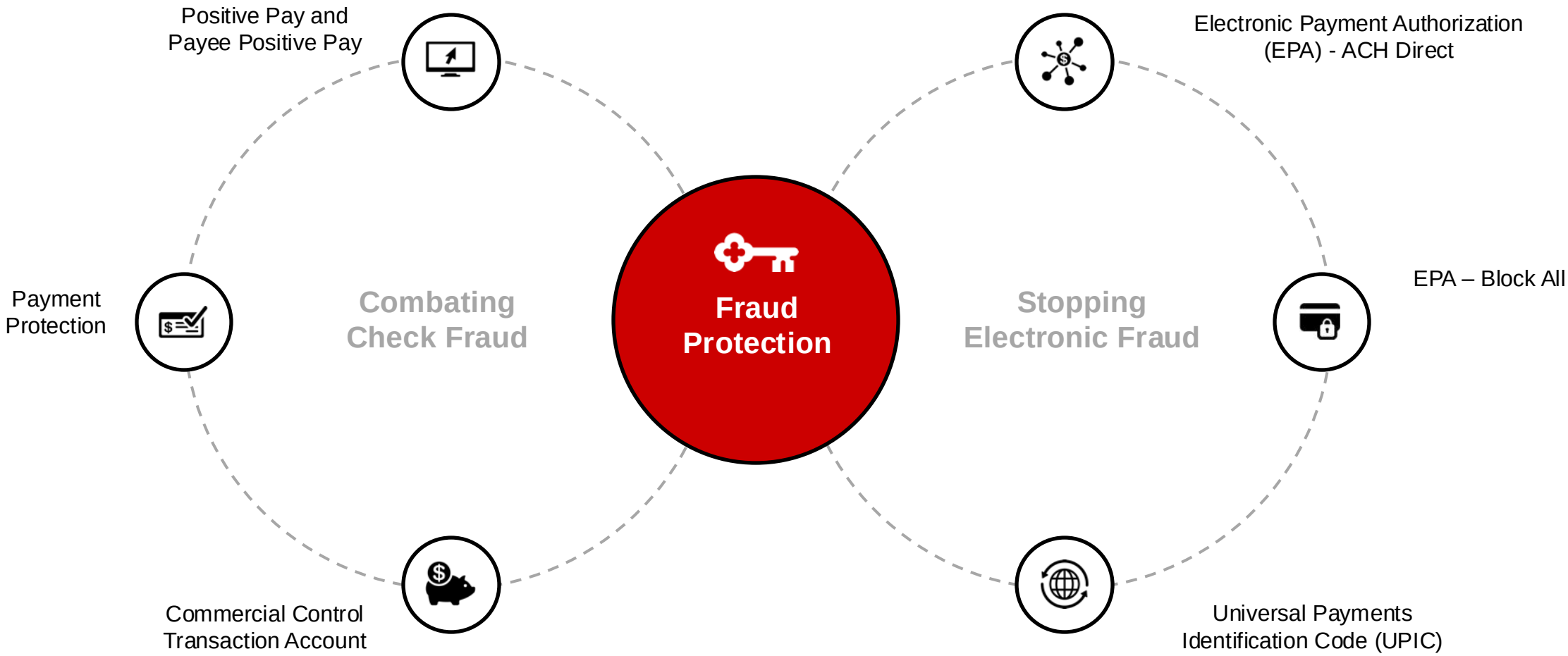
Monthly articles and quarterly client newsletters.

Client education opportunities focused on cyber trends and scams.

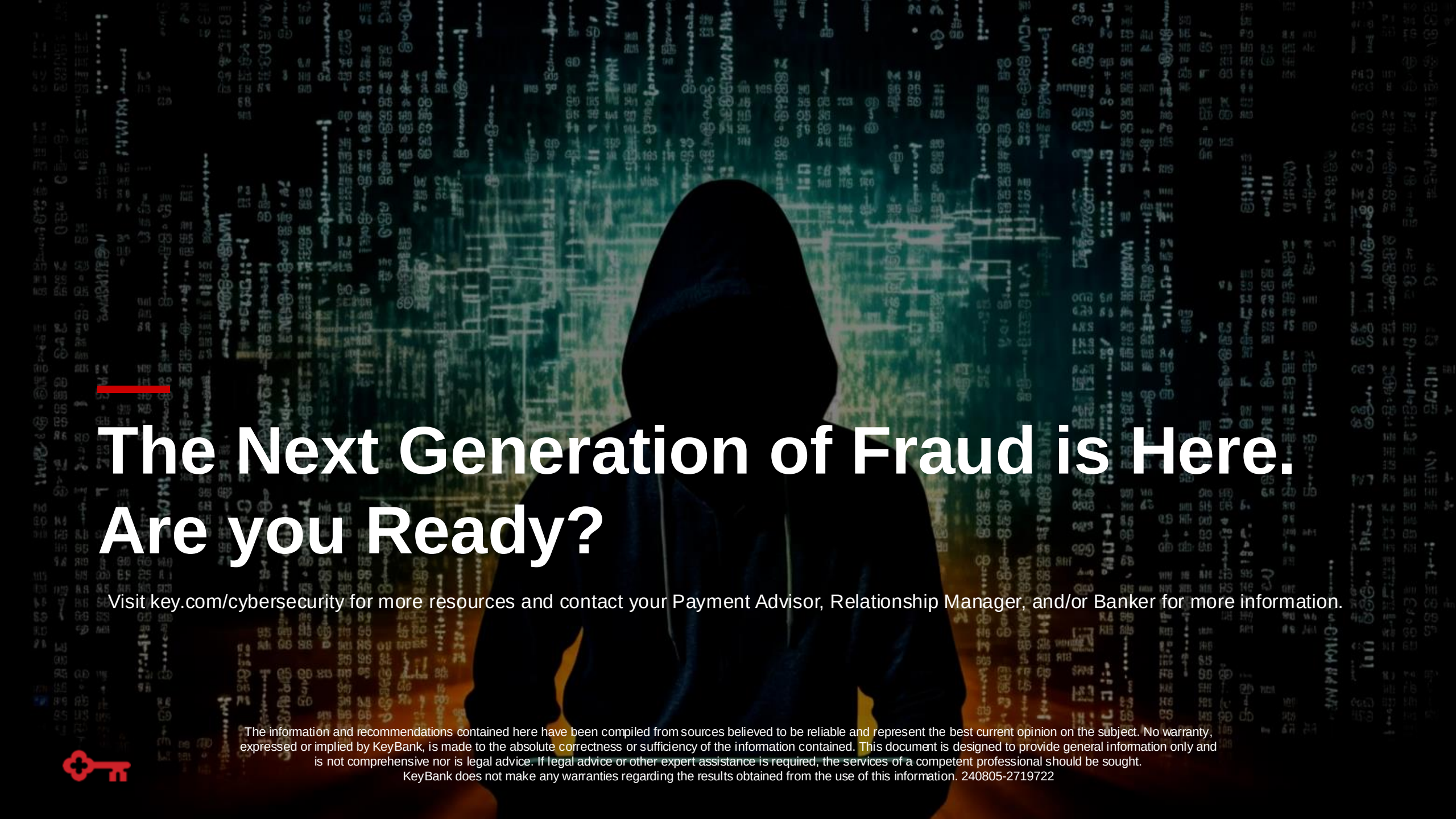
Ongoing compliance and fraud education for employees.

# What is KeyBank Doing?

KeyBank offers the following to help you bank safely and confidently with the following:



# Q&A



# The Next Generation of Fraud is Here. Are you Ready?

Visit key.com/cybersecurity for more resources and contact your Payment Advisor, Relationship Manager, and/or Banker for more information.