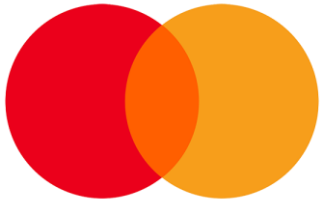
GLENBROOK

FraudWatch:
Cybersecurity Attacks



Q1 2023

About FraudWatch

- Quarterly briefings from Mastercard and Glenbrook
- Each briefing focuses on a specific payments risk or fraud topic
- Format
  - Trends and metrics related to the quarter's topic
  - A deep dive into a specific payments risk or fraud topic
  - Observations and takeaways

For any specific questions, please reach out to your Mastercard representative or fraudwatch@Mastercard.com

Speakers

Glenbrook

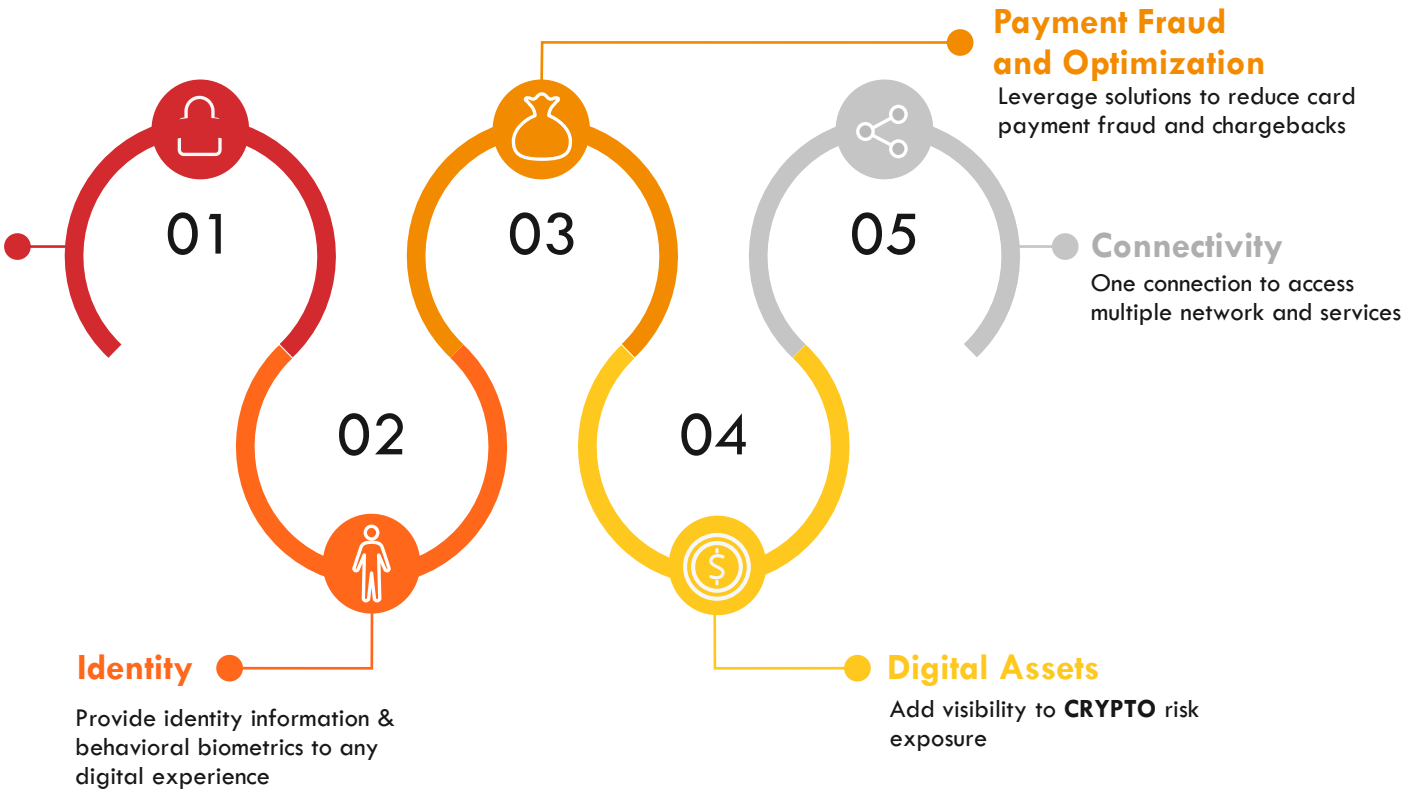
Chris's 25+ years in payments and risk management and C-suite experience brings Glenbrook's education programs to life and incorporates practical expertise in our client engagements

Andrew's experience at a NA Issuer and skilled analysis enables our team to isolate relevant insights critical to helping our clients

Mastercard

Mastercard Deputy Chief Security Officer Alissa "Dr. Jay" Abdullah leads a global team responsible for driving the future of security while also protecting Mastercard's information assets. Prior to Mastercard, she served as the Chief Information Security Officer of Xerox and Deputy Chief Information Officer of the White House.

Mastercard is evolving with the ecosystem…from securing transactions to protecting trust in every interaction while maintaining the best customer service

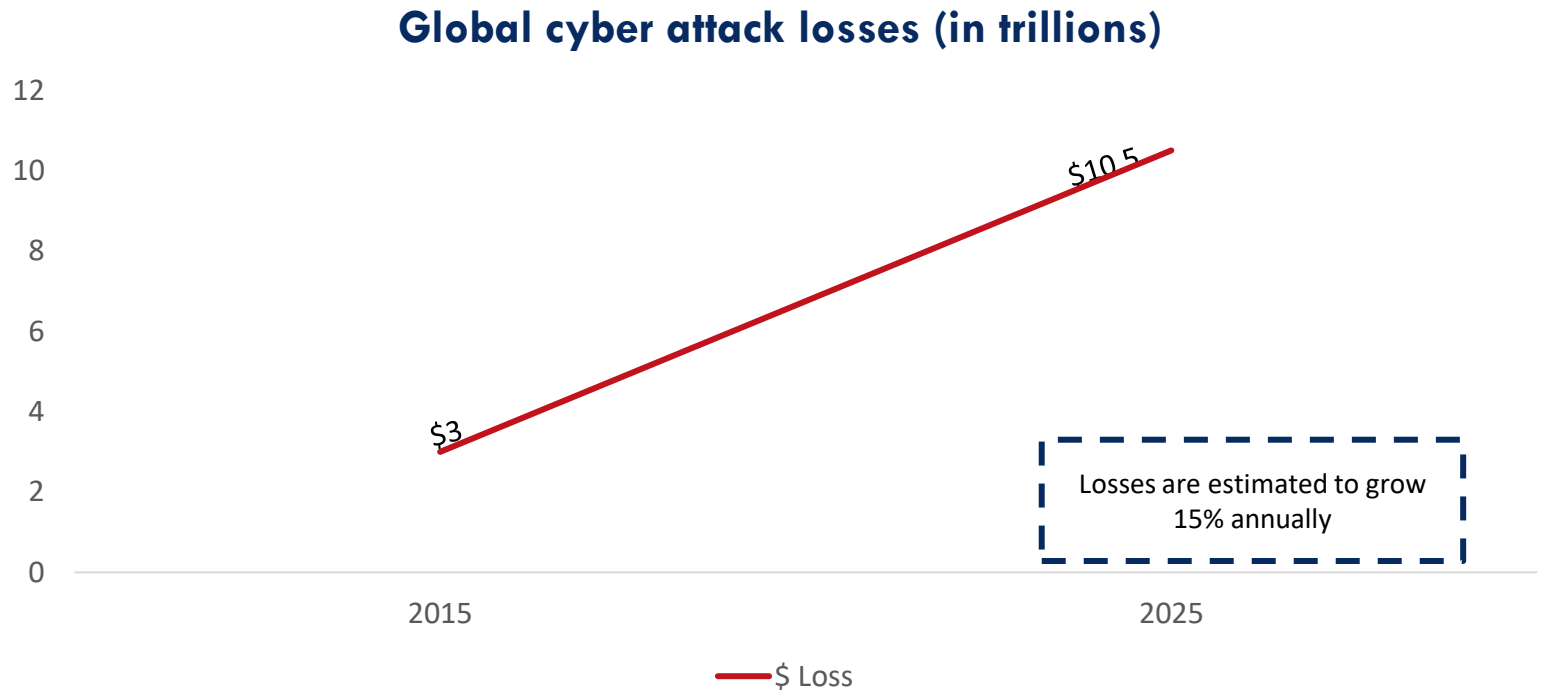


One trusted source for protection

GLENBROOK

Trends and Metrics

Cyber attacks: by the numbers



'The thing that worries me most is cyber risk'- Fed Chair Jerome Powell

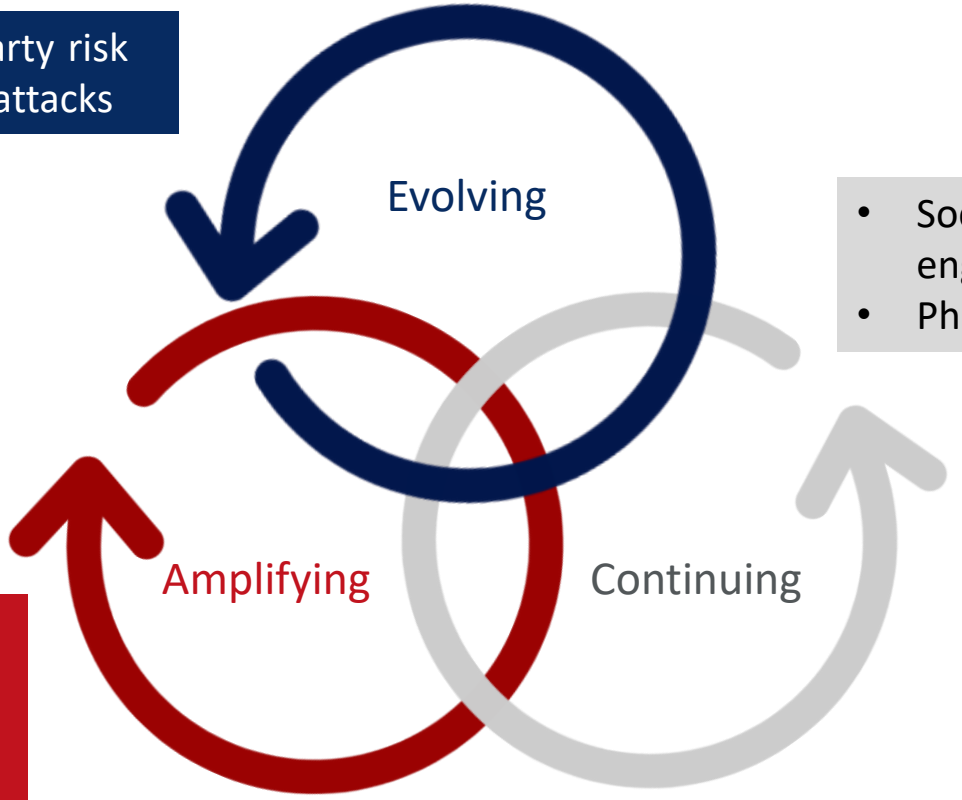
GLENBROOK

Source: McKinsey

Cyber attacks in 2023

Cyber risk typologies

- Third party risk
- Insider attacks



- Social engineering
- Phishing

- Zero day exploits
- Attacks on new payments

Tell us what you're thinking!

What type of threat or attack keeps you up at night?

Source: Freepik

Cyber attacks – what is continuing?

Professionalism of Attacker

- Organized attack and fraud rings
- Ransomware as a service

Broad Appeal of Payment Systems

- Cyber targets
- Mechanism for which fraud attacks happen
- Targeting new payments systems

Attack Tools

- Malware and ransomware
- Software and system exploits
- Insider access to critical systems
- Social engineering (esp. phishing)

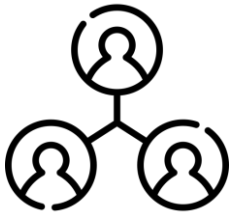
Cyber attacks – what is amplifying?

Critical role of employees

- As weak points, targets, and malicious actors

"We will see increases in insider risks, with attackers attempting to coerce and extort otherwise trustful insiders to commit malicious acts." – Phil Venables, Google Cloud

Critical role of third parties



- Several players in data processing flow

45%	Percentage of organizations that experienced a third-party security incident last year

Source: Glenbrook analysis, Prevalent

Cyber attacks – what is evolving?

Increased attacks on smaller companies

>30%	50%	70%
Percent of U.S. small businesses that have weak points for bad actors to exploit	Percent of U.S. small businesses that have experienced a cyber attack	Percent of all ransomware attacks affected small businesses in 2021

Source: Mastercard, McKinsey Forbes, Ransomware Taskforce

GLENBROOK

Cyberattack Scheme

Spotlight: meet Tom

Tom recently got promoted to manager, which means he has access to more sensitive company systems. He is so excited about his promotion that he posts about it on social media. He celebrates by attending an NBA game with coworkers and posts about it on social media.

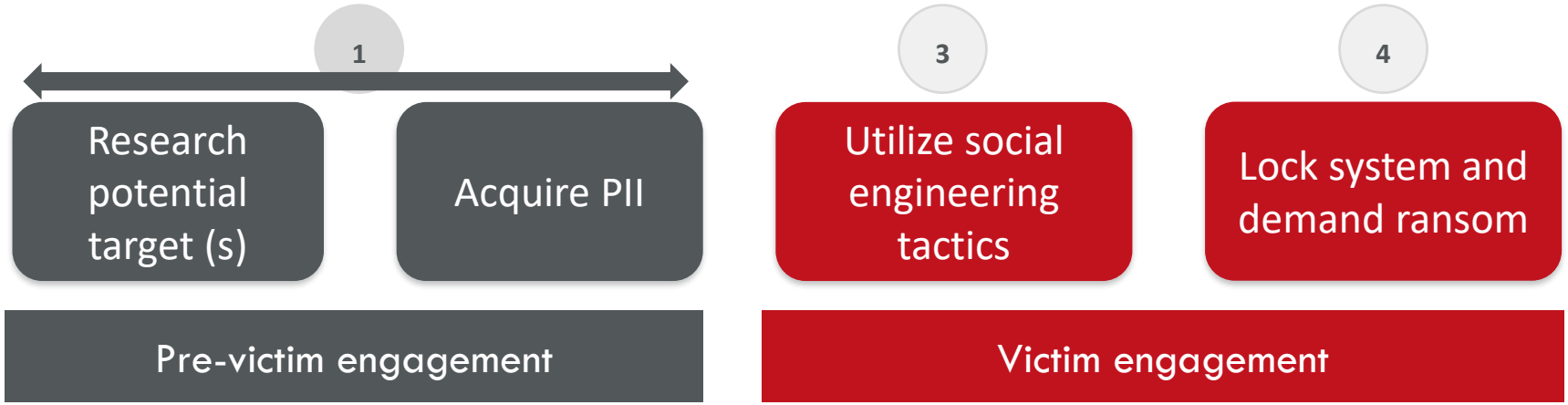
While chatting with colleagues, Tom receives an email from the company saying he won tickets to the NBA Finals because of his recent promotion. To receive the tickets, the email requires him to download and sign a document. After signing, he is prompted to install the app. He accepts but his computer immediately shuts off. Anxiously, he tries to reboot but to no avail. He then gets a message saying, “company and systems/data locked. $1M in bitcoin payment required to unlock.”

What happened?

Source: Glenbrook analysis
Photo Source: Designed by Freepik

Ransomware scheme process

Researching, acquiring personal data, and exploiting human emotions are critical for the ransomware journey



Obtain employee personal information by researching publicly available data (e.g., social media)

Capture data via data breaches, account takeover

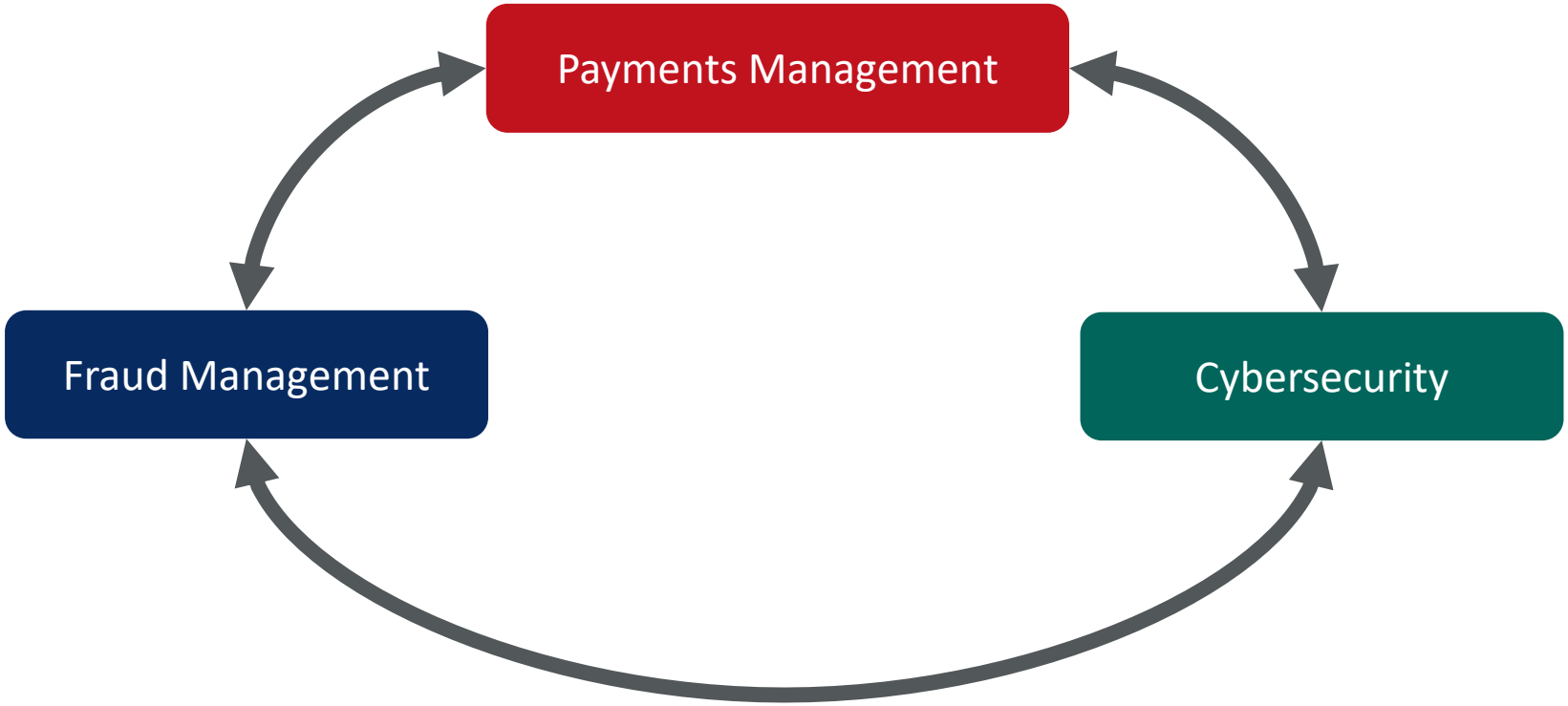
Utilize tactics such as phishing, vishing, etc.

Victim falls for attack, fraudster demands ransom

Time

Control Strategies

Organizational: Develop a cross-functional control strategy

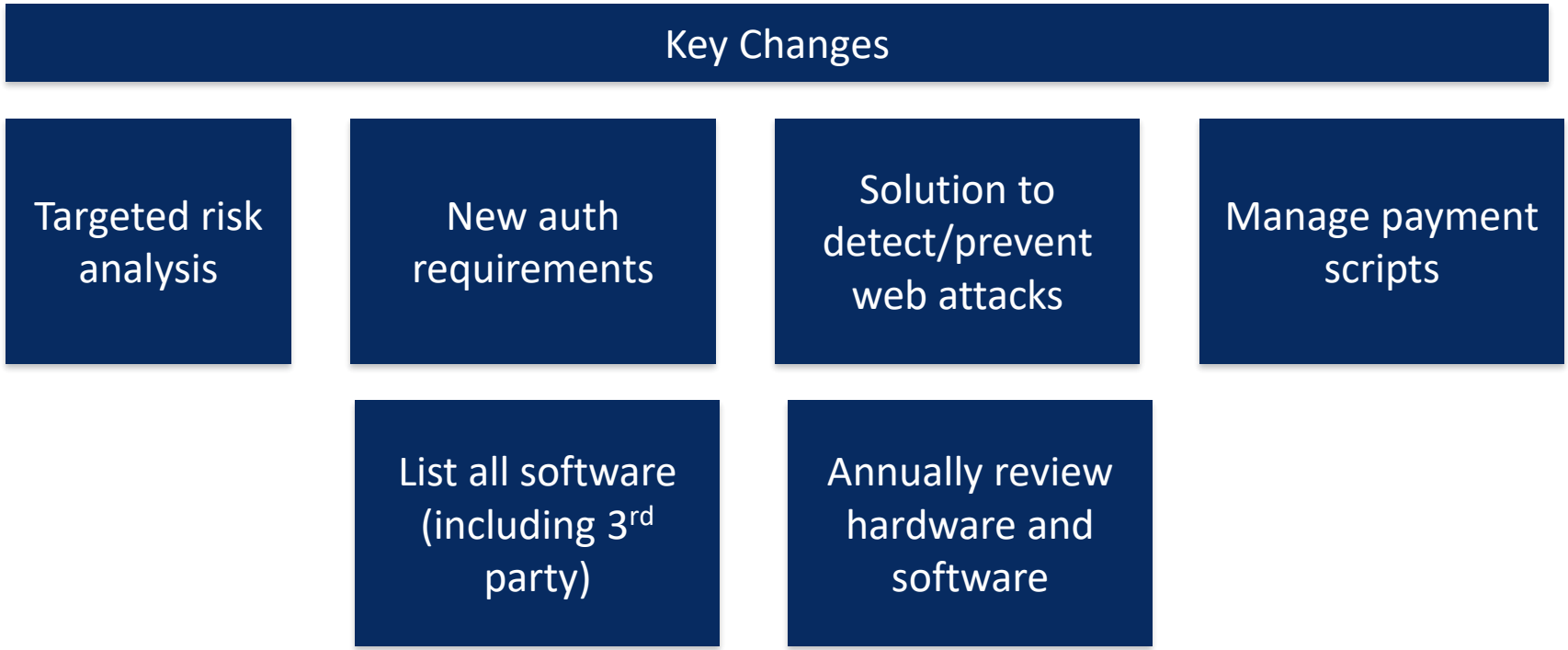


As fraud evolves, key business areas need to work cross functionally together in synergy to avoid silos

Business: Develop custom approaches to align with latest rules and regulations

Example: complying with PCI DSS 4.0

First major update since 2018; requires significant structural changes for payment stakeholders

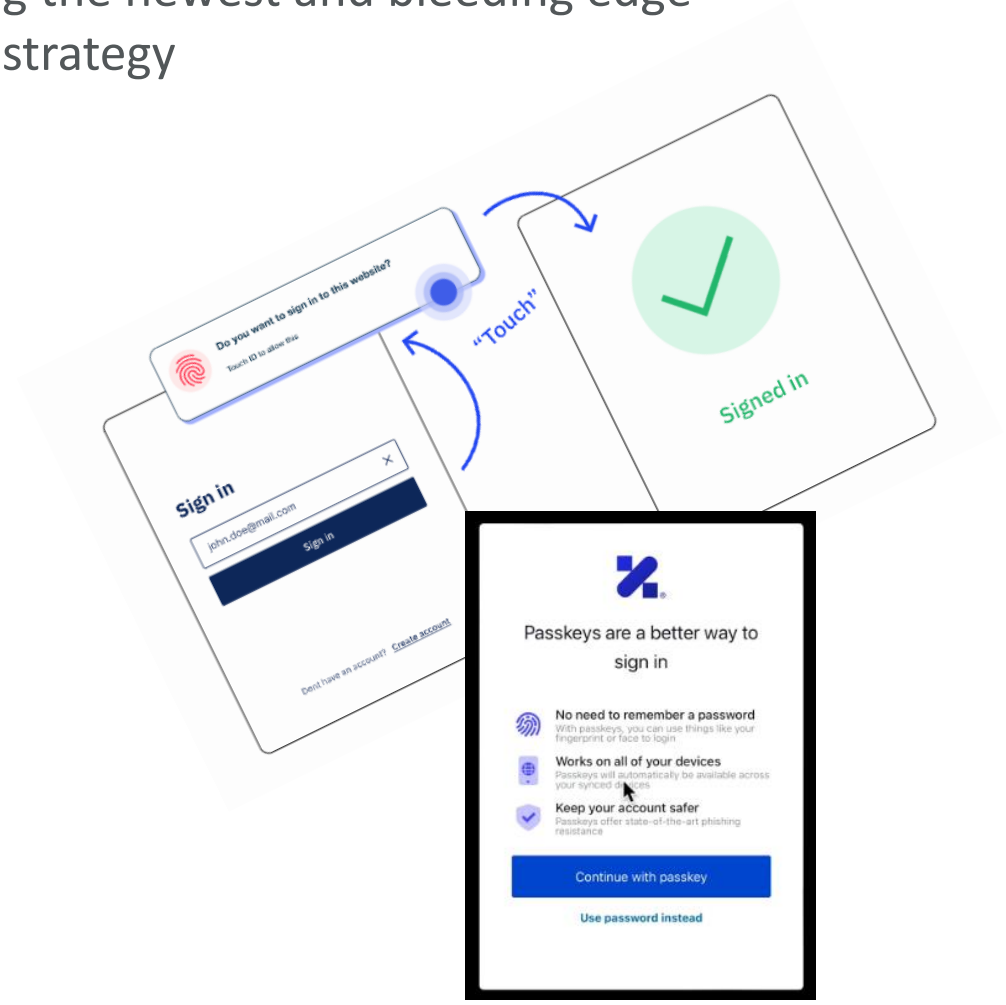


Source: Davis Wright Termaine

Technology: Stay abreast of evolving tools (Passkeys)

Organizations should start exploring the newest and bleeding edge technologies as part of their cyber strategy

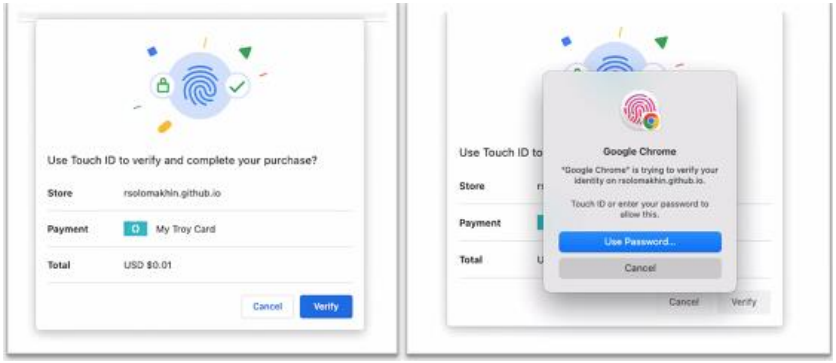
- Password replacement that provides a safer and faster login experience than traditional two factor authentication
- FIDO standard is being developed among big tech vendors
- Poised to be a widely used authentication method across website and apps

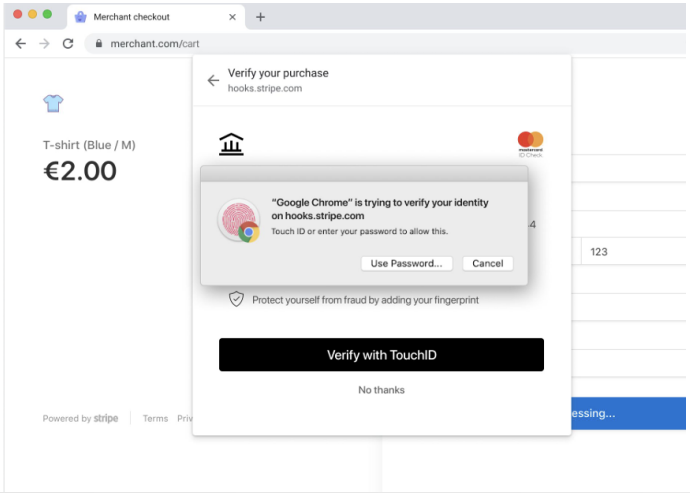


Technology: Stay abreast of evolving tools (Secure Payment Confirmation (SPC))

Organizations should start exploring the newest and bleeding edge technologies as part of their cyber strategy

- Utilizes WebAuthn standard to allow for biometric authentication at checkout flow
- Does not require users to download a separate app
- Nature of friction is very low as SPC providers a smoother end-user experience typical with day-to-day user actions





Should I get cyber insurance?

Cyber insurance is only a safety net in a multi-layered risk strategy

Cyberinsurance has evolved in recent years

Cyberinsurance can be a lifeline. However,

- Rising premiums have priced out certain businesses
- Insurance companies are reevaluating the cyber space

Cybercrime “will become uninsurable” – Mario Greco, CEO of Zurich Insurance

Source: Glenbrook analysis, Financial Times

GLENBROOK

Glenbrook Takeaways

Three recommendations

1. Consider not just your organizational risk but also your **third-party risk.**
2. Fraud is a major outcome of cyber risk. A **multi-pronged approach** must be used for both cybersecurity and fraud management, and both operations need to work hand in hand.
3. Compliance with standards (e.g., PCI) does not mean your environment is fully secure. Auditing is a point-in-time assessment and **cyber programs need to continually evolve**.

GLENBROOK

What is Mastercard doing?

Mastercard solutions

riskrecon mastercard

- Proactively monitors the cyber environment of any entity with an online presence to identify cyber risks and vulnerabilities before they can be exploited.
- 19+ million companies monitored globally
- Used by Sentara and Pfizer

NuData Security mastercard

- Offer cost efficient risk assessments for users based on behavior and device insights
- +20B in annual risk assessments and 4.5B devices monitored

EKATA mastercard

- Offers digital identity solutions to combat transaction fraud and reduce payment risk
- Used by 2,000 businesses worldwide

Cyber Quant

- Measures an organization's cyber risk, flag security gaps, and estimates impact of new cyber controls
- Creates personalized results and actionable recommendations

Source: Mastercard

GLENBROOK

Q&A