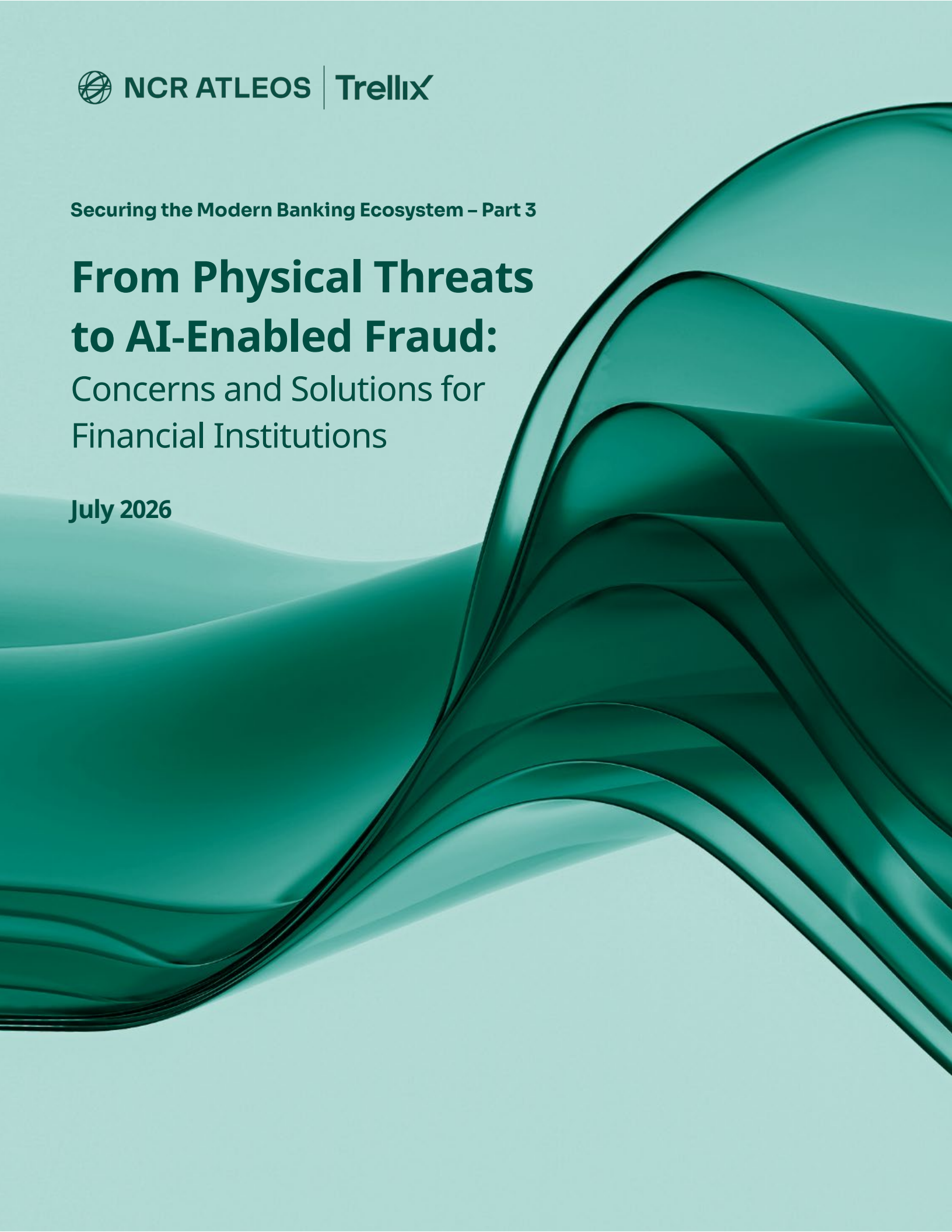


Securing the Modern Banking Ecosystem – Part 3

From Physical Threats to AI-Enabled Fraud:

Concerns and Solutions for
Financial Institutions

July 2026

A large, abstract graphic on the right side of the page. It consists of several overlapping, wavy, translucent teal shapes that create a sense of depth and movement, resembling liquid or flowing fabric. The colors range from a light teal to a darker, more saturated teal.

From Physical Threats to AI-Enabled Fraud:
Concerns and Solutions for Financial Institutions

Table of contents

Executive summary 2

AI-driven phishing and social engineering..... 3

Evolving attack vectors & ATM logical security..... 8

Final summary 10

Executive summary

Banks and ATM deployers face a convergence of physical crime, AI-driven social engineering, supply-chain fragility, and governance and behavioral gaps. The security landscape for Financial Institutions remains volatile and at times challenging.

In March, NCR Atleos and Trellix joined forces to host our first security summit at Abertay University Cyber Quarter in Dundee. By bringing together industry security experts, Financial Institutions and experts in cyber and fraud academia, we collectively asked questions and discussed real-time challenges on how to stay ahead of fraud and cyber-attacks, both aimed at the banking industry and beyond. We highlighted reporting frictions (e.g., data-sharing concerns under GDPR), over-reliance on reactive controls, and complex incidents that can often stretch resources for lengthy periods of time.

This white paper is one of four produced which outlines the key outputs from eight concern areas and the discussions that followed along with some key conclusions.

In the third whitepaper we look forward to how we secure tomorrow with a view on AI and evolving attack vectors, more specifically disaster recovery and security in the supply chain.

Trust & Threats The Shift in Physical Attacks Responsible Finance	Operational Resilience Disaster Recovery Supply Chain Security
Securing Tomorrow AI Driven Phishing & Social Engineering Evolving Attack Vectors	Covert & Coercive Risk Management Governance & Human Behavior

AI-driven phishing and social engineering

The rapid advancement of generative AI is materially transforming the threat landscape for ATM-focused financial institutions. Social engineering – already one of the most persistent sources of fraud loss – is becoming more scalable, more adaptive, and significantly harder to detect. For banks and ATM deployers, this shift has direct implications for logical security, fraud prevention, operational risk, and incident response models.

During the summit, several themes were discussed; here are some of the key points from this discussion.

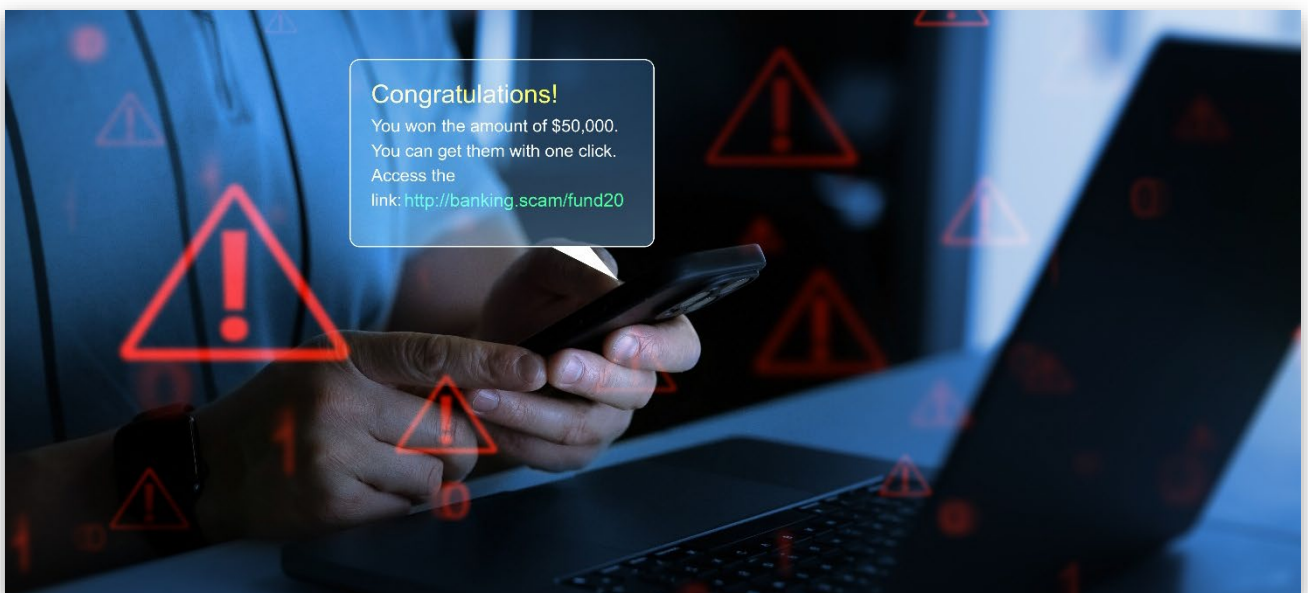
How AI is changing attacker tactics in ATM-related fraud

AI-driven phishing has become dramatically more sophisticated, with messages now able to mimic internal corporate language, operational communications, and vendor correspondence.

“Phishing emails are now clever enough to mimic exactly how current threats look — the wording, the links, the timing. Around Christmas, they bombard us.”

Jason Daniels

ATM & Cash Services Nationwide Building Society



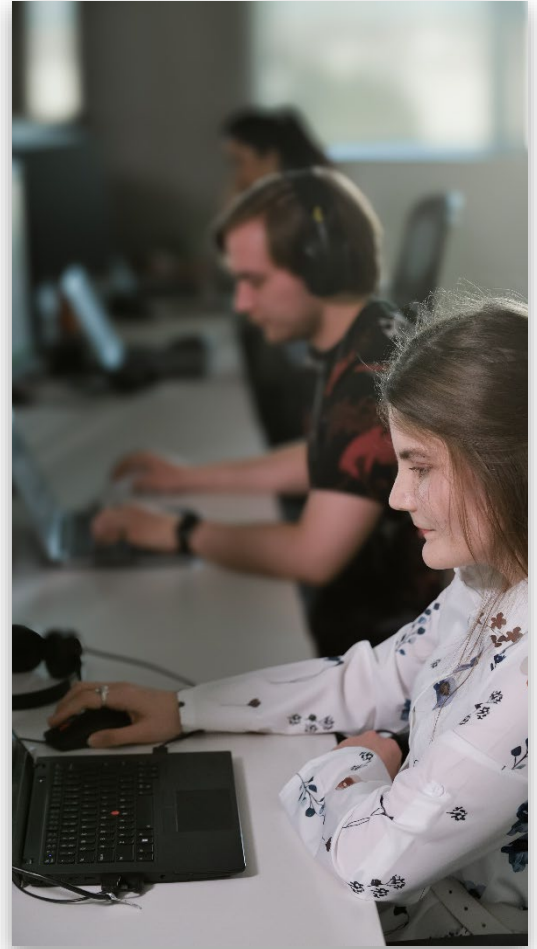
This increasing realism reduces the effectiveness of traditional user-awareness training. Attackers can tailor messages to seasonal behavior, operational workflows, and known stress points within ATM support teams which results in a raised likelihood that staff with privileged access may inadvertently engage with malicious content.

Targeting ATM operations teams

ATM support teams are particularly attractive targets because they hold access to:

- Remote Management interfaces
- Privileged credentials
- Maintenance workflows
- The ability to disable or override monitoring systems

Generative AI now enables attackers to impersonate third-party vendors, field engineers, or internal escalation teams with unprecedented accuracy. This creates opportunities for criminals to request configuration changes, authorize false site visits, or redirect support activity.



Convergence of digital and physical ATM threats

Although phishing is often seen as a digital-only threat, AI is enabling new forms of blended digital-physical fraud. A recent example described where fraudsters are faking both forms of ID, for example using AI to generate a realistic fake ID and a realistic deepfake video of themselves and submitting to verify identification.

“We had a live arrest, which was massive. Getting real-time intelligence to the guards meant we caught someone who’d been hitting multiple sites.”

Emma Keating
Software Security Strategy Manager, Tesco Insurance

This case illustrates the future direction of AI-enabled defense: real-time predictive models that correlate suspicious digital signals with physical behavior at ATMs.

“Imagine getting that information in real time from an AI system. That’s the end game — detecting it as it happens so we can stop the crime and get officers there.”

Emma Keating
Software Security Strategy Manager, Tesco Insurance

As criminals themselves adopt AI to disguise repeat patterns or automate parts of the attack lifecycle, the ability to rely purely on manual recognition or operator judgement will diminish.

Deepfakes, synthetic media, and the trust problem

Deepfake audio, video, and imagery represent a growing challenge for banks, where operational decision-making often depends on remote communication, recorded evidence, and identity verification.

The group noted concerns about the reliability of emerging watermarking technologies and asked the question, how soon before someone bypasses these AI watermarks and creates an AI version of them? That’s the worst-case scenario for us.

Even where watermarking exists, adoption is inconsistent, and global standardization is unlikely.

This lack of standardization creates an environment where synthetic content can circulate freely, but verification tools are fragmented and limited. Additionally, the group noted due to current watermark standards being optional for vendors and often proprietary that



watermarking itself could create user-trust issues. Indeed, a better solution might be to generate a unique signature that can be cryptographically signed by a device camera that creates it. For example, “proofmode” on android devices.

Authenticity assurance in ATM environments

However, despite global inconsistencies, banks and ATM operators manage environments where a closed ecosystem of trusted devices can support strong verification.

Digitally signed CCTV and ATM imagery

As previously outlined, there can be trust issues of authenticity of footage. A bank-controlled camera network could cryptographically sign footage at the point of capture, creating an unbroken chain of authenticity for fraud investigations.

“If your cameras are digitally signing the images they capture, at least you know the footage is genuine and hasn’t been modified.”

Alan Brown
CSM NCR Atleos



Markers of authenticity described above would support evidentiary requirements and ensure that fraud teams can rely on imagery even in an era of deepfake manipulation.

Such systems could embed:

- Device identity
- Timestamp and geolocation
- Frame-level image hashes
- Cryptographic signatures

This would cleanly separate content into trusted, untrusted, and ambiguous categories.

The future of internal imagery

Additionally, Donald Fraser, Engineering Director at NCR Atleos highlighted that in the future it may not be possible to verify and trust our own images. This underscores the urgency of developing internal authenticity frameworks before deepfakes and synthetic content fully penetrate criminal toolchains.

Implications for banks and ATM operators

The dialogue during the summit clearly outlined a direction: banks must update their logical security strategies to address the realities of AI-accelerated social engineering and blended fraud.

Key priorities include:

- Implementing adaptive, AI-aware phishing detection
- Strengthening verification for operational changes
- Protecting ATM operations teams with enhanced authentication requirements
- Developing predictive models for physical-digital threat correlation
- Creating secure, verifiable pipelines for imagery and video evidence

AI offers both risk and opportunity. As one participant noted, the strategic aim is to match attackers' speed with proactive defense.

In conclusion

AI-driven phishing and social engineering represent one of the most disruptive changes to ATM-related security in the last decade. Banks must anticipate a future where:

- Attackers operate at machine speed
- Social engineering is indistinguishable from legitimate communication
- Deepfakes erode the reliability of traditional verification
- Physical and digital threats converge in new ways

By implementing authenticity-verification mechanisms, strengthening cross-team intelligence flows, and adopting AI-native detection strategies, banks and ATM operators can significantly enhance resilience against emerging threats.

Evolving attack vectors & ATM logical security



As the ATM security landscape continues to mature, attackers are shifting their tactics to exploit newly emerging opportunities. The discussion shifted to highlight how adversaries are adapting in response to strengthened logical security measures, with particular emphasis on relay attacks, credential reuse, and the anticipated impact of quantum computing on cryptography.

Adaptation of techniques in response to stronger defenses

The conversation opened by exploring how attackers have altered their approaches following years of increased logical security enhancements. One of the clearest examples was the evolution of relay attacks, in which data from a compromised point-of-sale transaction is relayed in real time to an ATM-usable card.

These attacks demonstrate that even when card data is secured during traditional attack paths, adversaries can still circumvent the system by inserting themselves between trusted devices and processes.

Credential reuse: a growing weak link

Another prominent theme of the summit, was the role of password reuse across services, which continues to undermine even strong encryption schemes. The discussion emphasized that attackers increasingly exploit situations where people use the same password for multiple accounts—e.g., between a Google account and a bank account. This highlights a trend where compromise no longer necessarily requires defeating cryptography directly; instead, attackers lean on predictable or poor human practices to gain access.

Quantum computing as an emerging threat

A major focus of the session was the future impact of quantum computing on cryptographic protections. The group noted that attackers may increasingly exfiltrate encrypted data today, anticipating their ability to decrypt it later as quantum capabilities advance.

Quantum systems were described not as faster versions of classical computers, but as machines with fundamentally different predictive capabilities. This difference is particularly relevant for key-prediction, factorization, and the broader class of problems that underpin modern encryption.

The group noted that quantum computers are currently restricted to major tech companies and government research bodies, with public access limited to very basic single-qubit systems. Nevertheless, the future threat is significant, particularly as quantum methods could be used to reverse cryptographic keys by effectively performing all possible calculations simultaneously.

The role of standards and compliance

In response to these upcoming threats, the discussion highlighted the role of emerging standards—particularly from NIST—that aim to establish quantum-resistant cipher suites, including those already being incorporated into TLS 1.3. Compliance requirements, rather than purely security-driven initiatives, were recognized as likely to be the main driver forcing organizations to transition to these new standards.

Looking ahead

The team collectively recognized that while quantum threats are not yet operational for everyday attackers, the industry must stay ahead of upcoming developments. Early adoption of quantum-resistant standards, improved credential-hygiene controls, and continued monitoring of evolving attack techniques will be crucial for ATM systems to prepare for the next era of security challenges.



Final summary

The series of whitepapers highlight how financial institutions are facing a rapid convergence of physical ATM attacks, AI-enabled social engineering, and growing governance and human-behavior challenges, all intensified by regulatory and intelligence-sharing barriers. It argues that rising threat sophistication demands a shift toward ecosystem-wide collaboration, earlier security integration, and human-centered governance to build long-term resilience. Ultimately, securing the modern banking landscape requires coordinated action across technology, regulation, and culture.

NCR Atleos and Trellix would like to thank everyone who took part in the cyber summit sessions, for their willingness to participate, contribute, and collaborate so openly throughout the discussions.

