WHITE PAPER ● ADVISORS & TRANSFORMATION
NOVEMBER 2026

# Quantum computing and financial services

A position paper on disruption and strategic readiness



# Foreword

Quantum computing is a promising frontier technology, fast evolving and no longer a theoretical notion of the future. While yet to reach its apex, quantum computing is already posing a significant risk to enterprise financial security by challenging the essential elements of cryptographic trust.

While the precise timeline for cryptographically relevant quantum computing remains uncertain, some projections point to 2029-2030 as an important planning horizon for organizations preparing for a post-quantum future. In a post-quantum world, the foundational financial services assumptions as we know today might not hold, resulting in increased systemic risk and weakened digital and ecosystem trust. Bad actors are already exploiting these potential gaps, harvesting key financial data to store today and decrypt later when quantum computing advances.

This white paper explores the evolving risk profile with the inevitable arrival of quantum computing, the response it demands and the actions that are paramount to prepare for a post-quantum computing world. For financial institutions, (for example, banks, acquirers, PSPs, fintechs winning in a post-quantum computing would require making an early start on preparations, aiming for long-term resilience, cryptographic agility and adaptability. Mastercard Advisors & Transformation is bringing quantum readiness advisory to our customers, helping them to assess and prioritize risks and exposure, plan for remediation and execute post-quantum computing readiness programs.

**Marc Carolus**
Executive Vice President,
Advisors & Transformation
**Mastercard**

# Executive summary

Quantum computing is no longer a speculative technology on the distant horizon. While large-scale, fault-tolerant quantum computers are still emerging, the **disruptive impact on financial services security is already present today.** The industry must act not because quantum computers are fully operational, but because **the consequences of inaction are irreversible.**

The financial system is built on cryptographic trust: confidentiality of customer data, integrity of transactions, authentication of participants and non-repudiation across highly interconnected ecosystems. Quantum computing fundamentally challenges these foundations. Bad actors can exploit this asymmetry by **harvesting encrypted data today** with the intention of decrypting it in the future and creating immediate risk for long-lived financial data and systemic trust.

At the same time, quantum computing will also introduce long-term structural changes to how financial institutions operate, compete and collaborate. The response cannot be limited to a narrow technical upgrade. Instead, institutions must adopt a **two-horizon strategy:**

- **Near-term:** Reduce exposure, build cryptographic agility and prepare the organization for transition.

- **Long-term:** Redesign trust, risk and operating models to function in a post-quantum cryptography (PQC) environment.

The strategic question for financial leaders is no longer if quantum computing will matter, but **how early and how deliberately the institution prepares.**

# Quantum computing basics from a security perspective

From a security perspective, quantum computing represents a step-change in computational capability rather than an incremental improvement. Certain cryptographic protections that are computationally impractical to break today become tractable under quantum paradigms.

Modern financial services rely heavily on public-key cryptography to:

- establish secure connections,
- authenticate users, devices and systems,
- sign transactions and software and
- underpin public-key infrastructure (PKI) and digital trust frameworks.

Quantum computing undermines the mathematical assumptions on which many of these mechanisms are based. Symmetric cryptography is weakened but can be compensated for; **asymmetric cryptography and digital signatures are fundamentally challenged.**

Importantly, the industry does not need to predict the exact date of a "quantum breakthrough" for this to matter. The **risk profile shifts as soon as attackers believe quantum capability will eventually arrive,** because data and trust artifacts can be compromised retroactively.



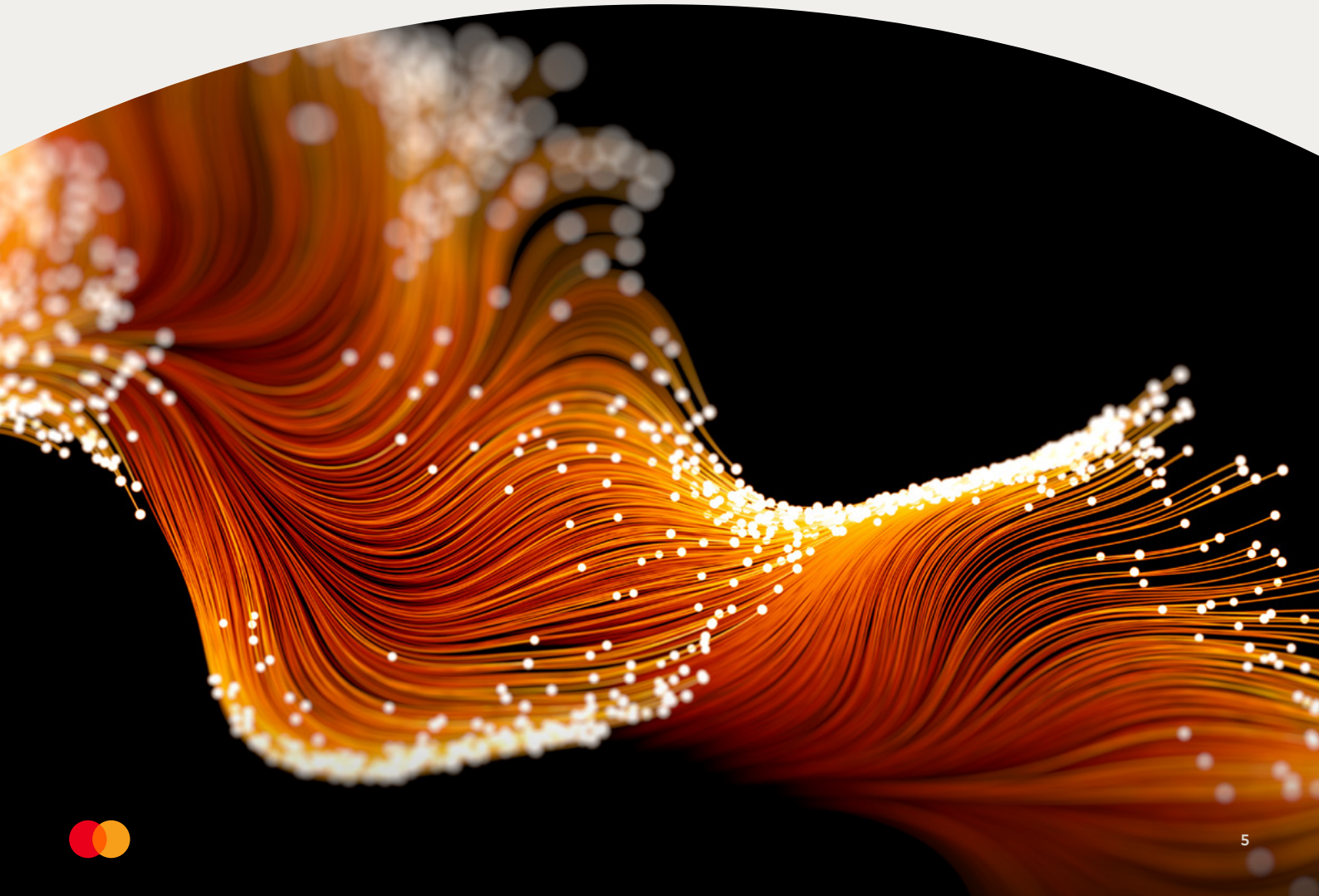
# Near-term risks: harvest now, decrypt later

The most immediate quantum-related threat to financial services is **"harvest now, decrypt later" (HNDL).**

Under HNDL, bad actors collect encrypted data today (such as network traffic, stored records, identity artifacts or transaction histories) with the expectation that future quantum capabilities will allow them to decrypt it. This creates several near-term consequences:

- **Confidentiality risk becomes time-dependent.** Data that must remain protected for years or decades is already at risk.
- **The breach horizon shifts forward.** A future quantum compromise can retroactively expose today's data, undermining legal, regulatory and reputational assurances.
- **Risk prioritization changes.** Long-lived, high-value financial data (customer identities, contracts, payment credentials, proprietary models) becomes disproportionately sensitive.

This means quantum risk is **not aligned to the arrival of quantum computers,** but to the **longevity of the data being protected today.**



# Long-term response: what breaks in a PQC world

In a post-quantum environment, several foundational assumptions of financial services no longer hold:

- **Digital trust is no longer implicit.** Existing certificates, signatures and trust anchors may no longer be reliable.
- **Non-repudiation is challenged.** The ability to prove the authenticity and integrity of historical transactions and records is weakened.
- **Ecosystem trust becomes fragile.** Financial services operate as networks (for example, banks, payment networks, merchants, fintechs and regulators). Weakness in one participant's cryptography can propagate across the system.
- **Systemic risk increases.** Uneven or uncoordinated migration creates disruptions in payments, settlement, identity and interoperability.

In practical terms, quantum computing turns cryptography from a **static control** into a **strategic dependency** that must evolve continuously.



# How to operate in a PQC world: strategic and business priorities

Operating in a PQC landscape requires financial institutions to move beyond a security model that assumes perfect data protection. In practice, **PQC resilience assumes that breaches will occur,** cryptographic trust will periodically be invalidated and historical data may be exposed retroactively.

The institutions that succeed will **design for resilience, adaptability and controlled recovery,** rather than absolute prevention.

## a. Shift from breach prevention to breach tolerance

In a PQC world, security strategy must evolve from "keeping data secret at all costs" to **limiting the business impact when secrecy fails.** This involves:

- Designing operating models that remain functional even when portions of data or trust infrastructure are compromised.
- Embedding assumptions of compromise into business continuity, legal posture and customer communications
- Treating cryptographic failure as a recoverable operational event, not a catastrophic one.

This mindset mirrors how financial institutions already manage fraud, credit risk and operational outages. Quantum risk should be treated with the same discipline.

## b. Decouple value from single points of data compromise

PQC winners will be those that **avoid concentrating decision making, value or competitive advantage in any single data set.**

Key strategic principles include:

- Data minimization by design: No single system, record or credential should expose the full economic or identity value of a customer, transaction or asset.
- Contextual decisioning: High risk actions should require corroboration across multiple data sources, systems or time windows.
- Progressive trust models: Trust is built dynamically using behavior, patterns and context, not solely static credentials or historical records.

In effect, data becomes less about stored truth and more about continuously validated evidence.

## c. Reframe risk through a data-longevity lens

Risk management must explicitly account for how long data and trust artifacts must remain secure, not just whether they are secure today. In a PQC environment, **confidence in historical data integrity may increasingly require risk-based validation rather than absolute assumption.** Institutions that thrive will be able to:

- Combine insights across **disparate internal and external data sources,** each with varying confidence levels.
- Operate effectively even when portions of historical data are questionable or exposed.
- Make decisions based on **patterns, correlations and real-time signals,** rather than reliance on any single authoritative record.

This inherently favors institutions with strong capabilities in:



**Advanced analytics and signal fusion**



**Cross-domain data governance**



**Real-time risk scoring and orchestration**

Fragmentation, when managed deliberately, becomes a strength rather than a liability.

### d. Redefine trust as dynamic, not static

PQC trust is not anchored permanently in certificates, keys or identities. Instead, it becomes:

- **Time-bound:** Trust decays and must be revalidated.
- **Contextual:** Trust depends on the situation, channel, behavior and risk profile.
- **Layered:** Multiple independent signals contribute to confidence.

From a business perspective, this means:

- Customer, merchant and counterparty trust will increasingly be assessed continuously.
- Products and services must be designed to function under varying confidence levels, with adaptive controls and experiences.
- Regulators and auditors will expect evidence of ongoing trust validation, not just point-in-time compliance.

### e. Embed quantum assumptions into governance and culture

Finally, operating in a PQC world requires cultural alignment:

- Executives and boards must understand that **quantum risk is systemic and long-lived,** not episodic.
- Risk appetite statements should explicitly account for cryptographic and retroactive exposure.
- Investment decisions must balance near-term efficiency with long-term resilience.

Institutions that normalize these assumptions early will adapt more smoothly as quantum disruption accelerates.

### f. Elevate quantum readiness to executive and board oversight

Quantum risk is not an IT problem; it is a **strategic, legal and systemic risk** that requires sustained executive sponsorship and governance.



# Conclusion

## What "good" preparation looks like

A credible post-quantum readiness program produces tangible, decision-enabling deliverables. Customers preparing for a post-quantum world can begin with focused Mastercard Advisors engagements that build readiness today and support long-term resilience.

1. **Quantum risk register**

   Prioritized business processes and datasets based on confidentiality lifetime and potential impact.

2. **Cryptographic discovery, inventory, and prioritization**

   Maintain continuous visibility into cryptographic assets and prioritize remediation based on business criticality, data sensitivity, and quantum exposure.

3. **Post-quantum transition roadmap**

   A phased plan aligned to business priorities, ecosystem dependencies and regulatory expectations.

4. **Cryptographic agility architecture principles**

   Guardrails that ensure new systems and vendors can adapt as cryptographic standards evolve.

5. **Executive and board reporting framework**

   Ongoing metrics and narrative that connect quantum readiness to business risk, resilience and strategic posture.

# How Mastercard can help



**Michael Yu**
Vice President, Security Consulting
**Mastercard**

**About Mastercard Advisors & Transformation**

Advisors & Transformation is the natural evolution of our consultancy offering: end-to-end partnership that combines deep payments, data and technology expertise with Mastercard network-level insight to help organizations optimize, innovate, grow and transform in a fast-changing world. Our deep connection to payments, data and operational systems helps you move faster from planning to rollout — with fewer handoffs and greater real-world relevance. We adopt a unified consulting model to align teams around shared goals and measurable impact, and we stay engaged to deliver transformation that sticks — not one-off recommendations. Our experts will be there for you through every stage of the process, enabling confident decisions with insights grounded in reality.

**About Mastercard Security Solutions Consulting**

Mastercard Security Solutions Consulting is helping shape the future of trust and security across the digital economy. As a trusted partner to financial institutions, merchants, fintechs, governments and ecosystem participants, we help our customers strengthen cyber resilience, combat fraud, modernize operational processes and navigate an evolving threat landscape.

We are focused on helping customers address challenges across cybersecurity, cyber risk, identity, cyber-fraud fusion, fraud prevention, disputes and chargeback operations, and merging risk domains. Combining Mastercard's network intelligence, technology capabilities and consulting expertise, we deliver data-driven strategies and practical solutions that help organizations reduce risk, improve performance and protect the consumers and businesses they serve. Through advisory, transformation and implementation services, we help customers build secure, resilient and future-ready enterprises and achieve measurable business outcomes.

# References and citations


1. NIST, Computer Security Resource Center, Announcing Approval of Three Federal Information Processing Standards (FIPS) for Post-Quantum Cryptography, August 13, 2024.

2. BIS, "Quantum computing and the financial system: opportunities and risks," October 9, 2024.

3. FS-ISAC, Post Quantum Cryptography resources.

4. Gov.UK, HM Treasury, "G7 Cyber Expert Group Statement on Advancing a Coordinated Roadmap for the Transition to Post-Quantum Cryptography in the Financial Sector: January 2026, January 13, 2026.

5. American Banker, "Why banks must treat quantum threats as a present risk," March 30, 2026.

6. Federal Reserve Bank, "'Harvest Now Decrypt Later': Examining Post-Quantum Cryptography and the Data Privacy Risks for Distributed Ledger Networks," September 2025.

7. World Economic Forum, "Global Risks Report 2026," January 14, 2026.

8. American Banker, "Citi: Banks face $3 trillion risk from quantum cyberattacks," February 12, 2026.

9. Finadium, "Europol, FS-ISAC release guidance for quantum migration in financial services, January 22, 2026.

