Quinte
Financial Technologies®

Post-Quantum Security

The Critical Gap in the Payments Ecosystem



19 Fulton Street
New York, New York 10038

(646) 813-0694
www.quinteft.com

INDEX

Executive Summary
03 | Background
Q-Day has Become a Business Risk

04-5 | Payment Rails are Exposed

06 | Tokenization is Not Enough
Legacy Systems Make the Transition Harder

07-8 | Regulators are Moving, But Execution is Still Early
Treasury’s Quantum-Readiness Task Force: A New Catalyst

09 | QR, Contactless, and Real-Time Payments Deserve Special Attention

10-11 | The Trillion-Dollar Security Race
What Payment Leaders Should Do Now

12 | Conclusion: Move from Awareness to Execution

13 | References

Executive Summary

Quantum risk is a growing business resilience concern for the payments industry. Increasingly, attackers are deploying a "harvest now, decrypt later" (HNDL) strategy, where they capture encrypted data today with the plan to crack it later when better decryption technology will make doing so far easier. While replacing vulnerable public-key cryptography can be an effective method for mitigating this risk, implementing it across financial institutions, processors, vendors, terminals, and digital-asset networks could take years. Leadership teams should look at inventorying cryptographic dependencies, prioritizing long-lived data and critical systems, building crypto-agility, and coordinating a phased migration with third parties. The objective is a governed, multi-year transition that protects trust, continuity, and regulatory readiness.

Background

Quantum computing is quickly moving from a future technical possibility to a practical business risk for today's payments industry. Citi Institute's January 2026 report, Quantum Threat: The Trillion-Dollar Security Race Is On, highlights the urgent problem that attackers can capture encrypted data today and decrypt it later once quantum technology matures. For an ecosystem built on trust, identity, authentication, and the uninterrupted movement of money, post-quantum security has evolved beyond the research lab and should be on leadership's agenda.

Q-Day has Become a Business Risk

"Q-Day" is the point at which quantum computers could break widely used public-key cryptography, including RSA and elliptic-curve cryptography (ECC). In its report, Citi estimates a **19%** to **34%** probability of widespread quantum-led attacks on this encryption by 2034, rising to **60%** to **82%** by 2044. The timing is uncertain, but the potential impact is severe. For financial institutions, that means treating quantum risk as a consideration in long-term resilience planning rather than leaving it as a theoretical concern.

Federal Reserve research on distributed ledger networks also highlights the risk of HNDL attacks where bad actors can obtain ledger replicas or related encrypted data, retain them, and use future cryptographically relevant quantum computers to reveal information that had previously been protected. For payment systems with data retention requirements exceeding seven years, including regulatory compliance, dispute resolution, and audit trails, the decryption window has already opened.

For this reason, payment institutions cannot wait for a visible quantum breakthrough. The longer the data lifespan, the wider the exposure; and the harder the migration path, the greater the urgency to act.

Payment Rails are Exposed

The payment rails exposure is best understood in three key layers: confidentiality risk from long-lived encrypted data, authentication risk from vulnerable signatures and certificates, and operational risk from slow migration across vendors, terminals, networks, and legacy platforms.

These layers cut across every major payment rail. Although the quantum threat will affect each differently, they all depend on cryptographic trust. Public-key cryptography, like RSA and ECC, helps authenticate systems, establish secure sessions, and verify transactions. A quantum computer capable of running Shor's algorithm* at scale could weaken those foundations, creating risks to confidentiality, authentication, and operational continuity across the entire payments ecosystem.

ACH and Instant-Payment Rails

Systems such as ACH and FedNow depend on TLS, PKI, and clearing-network authentication. Symmetric encryption can remain strong with sufficient key sizes, but the asymmetric layer used for handshakes, certificates, code signing, and identity is far more vulnerable.

** Shor's algorithm is a quantum computing algorithm that could efficiently break widely used public-key cryptographic systems such as RSA and elliptic-curve cryptography.*

Checks

While physical checks may seem analog, modern check processing depends on digital image clearing, signature verification, and backend authentication systems. Those systems inherit the same cryptographic dependencies as other payment rails and should be included in any post-quantum inventory.

Cryptocurrency and Digital Assets

For the blockchain, quantum computing presents a much bigger threat to digital signatures than the blockchain record itself. Publicly visible keys create exposure, as a future quantum computer could potentially derive private keys and sign fraudulent transactions through this data.

The Citi report estimates that around **25%** of Bitcoin, or roughly **4.5** million to **6.7** million BTC, may already be quantum exposed due to reused addresses or otherwise exposed public keys. While the exposure is even higher for some newer blockchains, including Ethereum and Solana, these ecosystems may be able to move faster given their more flexible governance and upgrade paths.

Cards, Wallets, and ATMs

EMV cards, NFC payments, mobile wallets, and ATM networks rely on cryptography to establish trust between credentials, devices, terminals, and networks. If signature schemes are compromised, attackers can impersonate credentials or forge authorization flows that were previously considered secure.

Additionally, some contactless payment technologies also depend on asymmetric cryptography in parts of their authentication and certification chains, making offline authentication and certificate validation important areas for post-quantum review.



Tokenization is Not Enough

Tokenization reduces the exposure of raw payment credentials, but it does not eliminate cryptographic risk. Every token still relies on keys, signatures, certificates, and validation chains to prove that it is genuine and being used by the right party. If those underlying mechanisms become vulnerable, tokenization may limit the data exposed without preventing actual impersonation, forgery, or misuse. Although it is an important control, it is not a substitute for post-quantum migration.

This is especially critical for mobile wallets, network tokens, digital-banking credentials, and tokenized settlement assets. Services such as Apple Pay and Google Pay rely on layered authentication, including tokens, certificates, and asymmetric cryptography. A future quantum attack on vulnerable signature or key-exchange mechanisms could weaken parts of those trust chains and increase the risk of credential misuse or fraudulent transactions. Therefore, tokenization and post-quantum migration should be treated as complementary priorities, rather than interchangeable substitutes.

Legacy Systems Make the Transition Harder

Major technology transitions, such as the move from magnetic stripes to EMV chips, are not new to the payments industry. Post-quantum migration, however, is far different. It touches certificates, key exchange, signing, hardware modules, terminals, ATMs, network protocols, vendor platforms, and operational processes simultaneously.

The challenge lies in choosing the right algorithms and making them work inside systems with tight payload limits, latency requirements, certification cycles, and old infrastructure. Hybrid cryptography, which runs classical and quantum-resistant algorithms in parallel, offers the most realistic transition path. However, it also requires crypto-agility that many legacy environments were never designed to support.

Many payment systems still run on legacy infrastructure, including core platforms written in COBOL and connected to long-lived ATM estates. This means the main barrier to quantum-safe payments is not the mathematics alone. New algorithms must fit within existing payload limits, meet strict latency requirements, and pass hardware and network certification. In legacy environments, even a small cryptographic change can trigger extensive testing, vendor coordination, and replacement cycles.

Regulators are Moving, But Execution is Still Early

While regulators are increasingly moving the issue up the agenda, the process is slow and the implementation gap is wide. The G7 Cyber Expert Group roadmap encourages coordinated migration across the financial sector. Europol's report gives institutions a practical way to prioritize systems based on quantum risk and migration time. NIST has already finalized its first post-quantum cryptography (PQC) standards, including ML-KEM for key establishment and ML-DSA for digital signatures.

Though important to the process, guidance is not the same as execution. Financial institutions still need complete cryptographic inventories, vendor readiness plans, testing environments, migration funding, board-level ownership, and clear timelines for high-risk systems.

However, regulatory direction is becoming clearer. NIST has standardized core post-quantum algorithms through FIPS 203, 204, and 205. U.S. federal timelines indicate that high-risk systems should move first, whereas the European Union is encouraging member states to develop national PQC transition strategies. For institutions, the leadership implication is direct: quantum readiness is likely to become a key component of supervisory expectations, third-party risk management, investment planning, and technology resilience.

Treasury's Quantum-Readiness Task Force: A New Catalyst

In August 2026, the U.S. Treasury Department announced a Quantum-Readiness Task Force to coordinate the financial sector's transition to quantum-safe technology. The task force is a public–private initiative that brings together government officials, financial institutions, financial market infrastructures, technology providers, and other industry leaders with the stated purpose of ensuring that the shift to post-quantum cryptography happens in an "orderly and operationally resilient manner." This move signals a shift from broad awareness toward sector-level coordination, with particular attention to operational resilience, third-party dependencies, and digital assets.

The Treasury's focus is explicitly practical and risk-based, highlighting:

- Identifying critical dependencies across the payments and financial ecosystem
- Improving cryptographic agility so algorithms can be changed without major disruption
- Promoting interoperability between institutions, vendors, and platforms
- Strengthening operational resilience in the face of quantum-related cyber risk
- Addressing implementation challenges tied to third-party dependencies and digital assets

The task force will operate through three workstreams:

1. Sector Alignment & PQC Transition – coordinating industry-wide migration practices and timelines.

2. Third-Party & Vendor Readiness – ensuring that cloud providers, software vendors, hardware security module (HSM) manufacturers, network-equipment suppliers, and other technology partners can support PQC in the products and services they provide to financial institutions.

3. Digital Assets & Emerging Technology Risk – examining how quantum computing affects cryptocurrencies, tokenized assets, and other emerging financial technologies.

This initiative formalizes the practical reality that no payment institution can become quantum-ready on its own. A bank or credit union may complete its internal migration and still remain exposed through a processor, gateway, cloud provider, vendor, or market infrastructure that has not kept pace. By making third-party readiness a dedicated workstream, the Treasury is acknowledging that the payments ecosystem is only as resilient as its weakest cryptographic dependency.

For boards and CISOs, the task force sends a clear signal: quantum readiness is moving from a technical project to a supervisory expectation. Institutions that cannot demonstrate progress on cryptographic inventories, vendor assessments, and migration planning may face heightened scrutiny in resilience exams, third-party risk reviews, and technology audits.

QR, Contactless, and Real-Time Payments Deserve Special Attention



QR-based and contactless payments create a particularly challenging risk profile as they combine scale, speed, offline validation, device trust, and consumer-facing authentication. Quantum computing does not make QR codes or NFC obsolete; rather, the issue is whether the signature and validation chains behind those experiences remain trustworthy.

India's UPI, mobile wallets, NFC payments, card-present transactions, and similar real-time systems all depend on high-confidence authentication at massive scale. Any migration plan must therefore look beyond central infrastructure and include terminals, mobile devices, token services, QR payload validation, and fallback flows.

Researchers have shown attacks that can enable fraudulent high-value contactless transactions by exploiting gaps in how some devices confirm user intent. In these scenarios, a device may treat proximity and an earlier biometric unlock as sufficient proof that the customer approved the payment. This creates an opportunity for relay, or "wormhole," attacks where transaction messages are forwarded between a legitimate device and a distant payment terminal. Such attacks have been demonstrated against both Apple Pay and Google Pay. While not actual quantum attacks, they do illustrate how quickly weaknesses in authentication and trust chains can become payment fraud risks.

Standards bodies including GSMA, IETF, 3GPP, and ICAO are all working to incorporate post-quantum cryptography into relevant protocols and guidance, particularly where long data lifecycles, high criticality, and significant potential harm converge. For payments, the connected areas that should be particularly monitored include eSIM management for mobile wallets, identity documents used in KYC and AML processes, and mobile communications that support device and payment authentication. These dependencies must be included in cryptographic inventories and vendor-readiness assessments.

The Trillion-Dollar Security Race

Additionally, Citi's report illustrates the scale of the risk through a severe disruption scenario. The research suggests that if a quantum-enabled attack blocked a major U.S. financial institution's access to Fedwire for just one day, the resulting disruption could place as much as **$2.0 - $3.3** trillion of economic activity at risk, or about **10%-17%** of annual U.S. GDP. Though this exact scenario may never occur, it highlights how deeply cryptography is embedded in payments, identity, messaging, and settlement, and why a successful quantum attack could threaten wider financial stability.

The total global payment card volume reached **$51.9** trillion in 2024, with the reported industry fraud losses at **$33.41** billion. These losses are projected to reach **$41.06** billion by 2030, with cumulative losses over the next decade estimated at **$407.6** billion. These figures showcase the scale of today's payment environment rather than any incremental loss caused by quantum computing. Quantum capabilities could nevertheless reshape both defense and attack. Advanced algorithms may help institutions identify suspicious transaction patterns faster, while sophisticated adversaries could possibly use similar capabilities to explore vulnerable networks more efficiently.

What Payment Leaders Should Do Now

Rather than a single action, Citi frames readiness as a five-step discipline: identify, prioritize, enable crypto-agility, migrate, and sustain. For payment leaders, this framework is a very practical approach as it treats PQC migration as a multi-year operating program rather than a one-time technology upgrade.

1. Identify - Build a complete inventory of where public-key cryptography is used across applications, infrastructure, payment platforms, identity systems, certificates, APIs, HSMs, and vendor services.

2. Prioritize - Focus first on identity systems, payment infrastructure, digital signatures, long-lived sensitive data, and systems where operational disruption would create severe business or systemic impact.

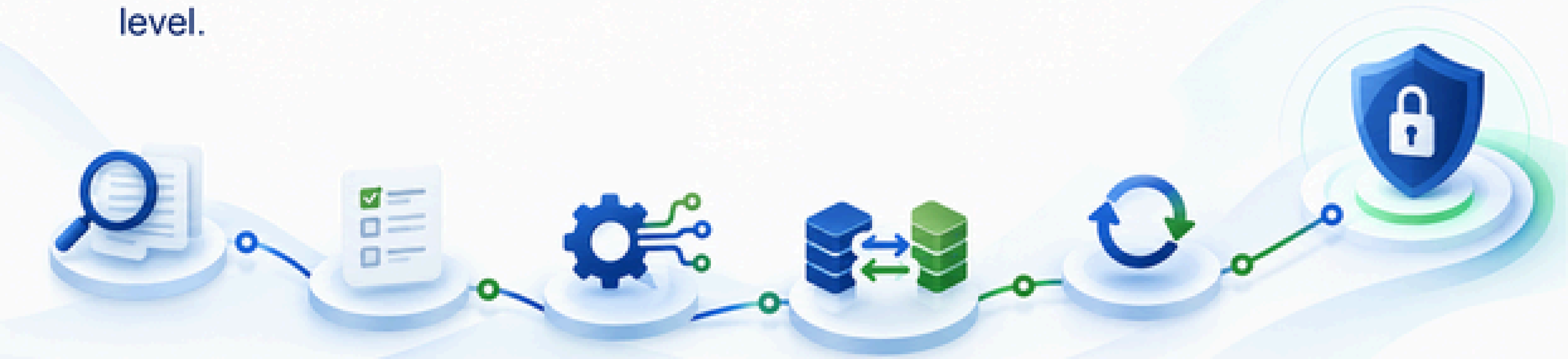
3. Enable crypto-agility - Design systems so algorithms, certificates, protocols, and key-management processes can change quickly without major reengineering. This is paramount because standards, vendor support, and implementation guidance will continue to evolve.

4. Migrate in phases - Use hybrid cryptography where appropriate, test performance early and often, and sequence migration around critical systems, vendor dependencies, certification cycles, and regulatory milestones. Algorithm and parameter choices should reflect the sensitivity and required lifetime of the data, the system's performance constraints, applicable regulatory guidance, and the evolving recommendations of standards bodies.

5. Sustain resilience - Keep management, key rotation, monitoring, vendor readiness, and emerging PQC standards under active governance. Quantum readiness should become part of routine cyber resilience, not a one-off project.

Leadership decisions required: appoint an executive sponsor for post-quantum readiness; fund a complete cryptographic inventory and risk assessment; prioritize long-lived sensitive data, identity systems, payment infrastructure, and digital signatures; require critical vendors to disclose their migration plans; establish milestones for crypto-agility, hybrid testing, and phased deployment; and include quantum readiness in board-level cyber-resilience reporting.

G+D's feasibility study with the German Federal Printing Office, one of the world's first functional demonstrators of a national ID card featuring both classical and post-quantum cryptography, proves that hybrid PQC deployment is technically achievable. This is the model payment networks must emulate, running classical and quantum-resistant algorithms in parallel, as endorsed by NCSC, ANSSI, BSI, and demonstrated in BIS Project Leap at the central-bank level.



Conclusion: Move from Awareness to Execution

Post-quantum security is ultimately about protecting both the trust in and the integrity of the systems that move money every second around the globe. The payments ecosystem cannot afford to wait until quantum computing becomes a visible operational crisis. By then, valuable data may already have been harvested, regulators may be asking for evidence of readiness, and the most complex legacy systems will still be years from migration.

Early action is likely to cost far less than responding late. Leaders must begin with a clear view of their cryptographic estate, focus investment on the systems and data that matter most, build crypto-agility into technology decisions, and hold critical vendors to the same standard. Post-quantum readiness must be governed as a multi-year business transformation, not left as a future security project.

The industry is already moving: research is advancing, investment is rising, standards are maturing, and governments and institutions are setting migration targets. As G+D observed in July 2026, preparing for the quantum era "is not an option for tomorrow; it has already begun." For leadership teams, the message is clear: make the transition deliberately now, rather than under pressure later.

The strategic choice is clear: lead a coordinated post-quantum migration or accept growing exposure as today's cryptography ages. Success will depend less on predicting the exact arrival of Q-Day than on aligning governance, funding, technology, and partners early enough to protect long-lived data and the trust mechanisms on which modern payments depend.



Authors: Sriram Natarajan and Paresh Ashara

Sriram Natarajan is President of Quinte Financial Technologies Pvt. Ltd. and has more than 30 years of experience in financial services, including work with credit unions and payment processors. His career in credit and risk includes leadership roles at American Express, HSBC, the National Bank of Kuwait, and GE Money. He is a Certified Public Accountant, Chartered Global Management Accountant, and Certified Fraud Examiner.

Paresh Ashara is Vice President at Quinte Financial Technologies Pvt. Ltd., where he leads the Data Analytics, AI, and Automation solutions and services business. He has more than 27 years of experience in IT services and product engineering across the banking, financial services, and insurance sector. His professional interests include data, advanced analytics, generative AI, and agentic AI.

References

[1] Citi Institute | Quantum Threat: The Trillion-Dollar Security Race Is On, January 2026 | https://www.citigroup.com/rcs/citigpa/storage/-public/Citi_Institute_Quantum_Threat.pdf

[2] NIST CSRC | Post-Quantum Cryptography | https://csrc.nist.gov/projects/post-quantum-cryptography

[3] NIST | First finalized post-quantum encryption standards | https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards

[4] U.S. Treasury | G7 Cyber Expert Group roadmap for post-quantum cryptography in the financial sector | https://home.treasury.gov-/system/files/136/G7-CEG-Quantum-Roadmap.pdf

[5] Europol | Prioritising post-quantum cryptography migration activities in financial services | https://www.europol.europa.eu/publications-events/publications/prioritising-post-quantum-cryptography-migration-activities-in-financial-services

[6] Federal Reserve | Harvest Now, Decrypt Later and Data Privacy Risks for Distributed Ledger Networks | https://www.federalreserve.go/ecores/fes/haest-now-dcrypt-laer-examining-post-quantum-cryptography-and-the-data-privacy-risks-for-distributed-ledger-networks.htm

[7] Hillary Muzenda and Belinda Ndlovu | Journal of Information Security article on post-quantum migration | https://journal-isi.org/index-.php/isi/article/view/1477

[8] PostQuantum | FINMA quantum guidance | https://postquantum.com/security-pqc/finma-quantum-guidance/

[9] Sébastien Rousseau] Securing the Ledger | https://sebastienrousseau.com/2026-05-14-securing-the-ledger-post-quantum-migration-corporate-finance/

[10] Andrea Fortuna | Contactless payment security | https://andreafortuna.org/2026/04/20/contactless-payment-security/

[11] Business Wire | TechCreate Group and pQCee quantum-safe QR hybrid POS terminal | https://www.business-wire.com/news/home/20260420365518/en/Crate-Group-Ltd.-and-pQCee-Intend-to-Collaborate-on-One-of-the-First-Quantum-Safe-QR-Hybrid-POS-Terminal

[12] G + D | Post-Quantum Cryptography: Act Now | https://www.gi-de.com/en/about-us/press/press-releases/when-quantum-computers-become-a-reality-from-future-concern-to-present-priority

[13] Bank Info Security | Treasury Launches Quantum Task Force for Financial Sector | https://www.bankinfosecurity.com/treasury-launches-quantum-task-force-for-financial-sector-a-32689

Quinte Financial Technologies®