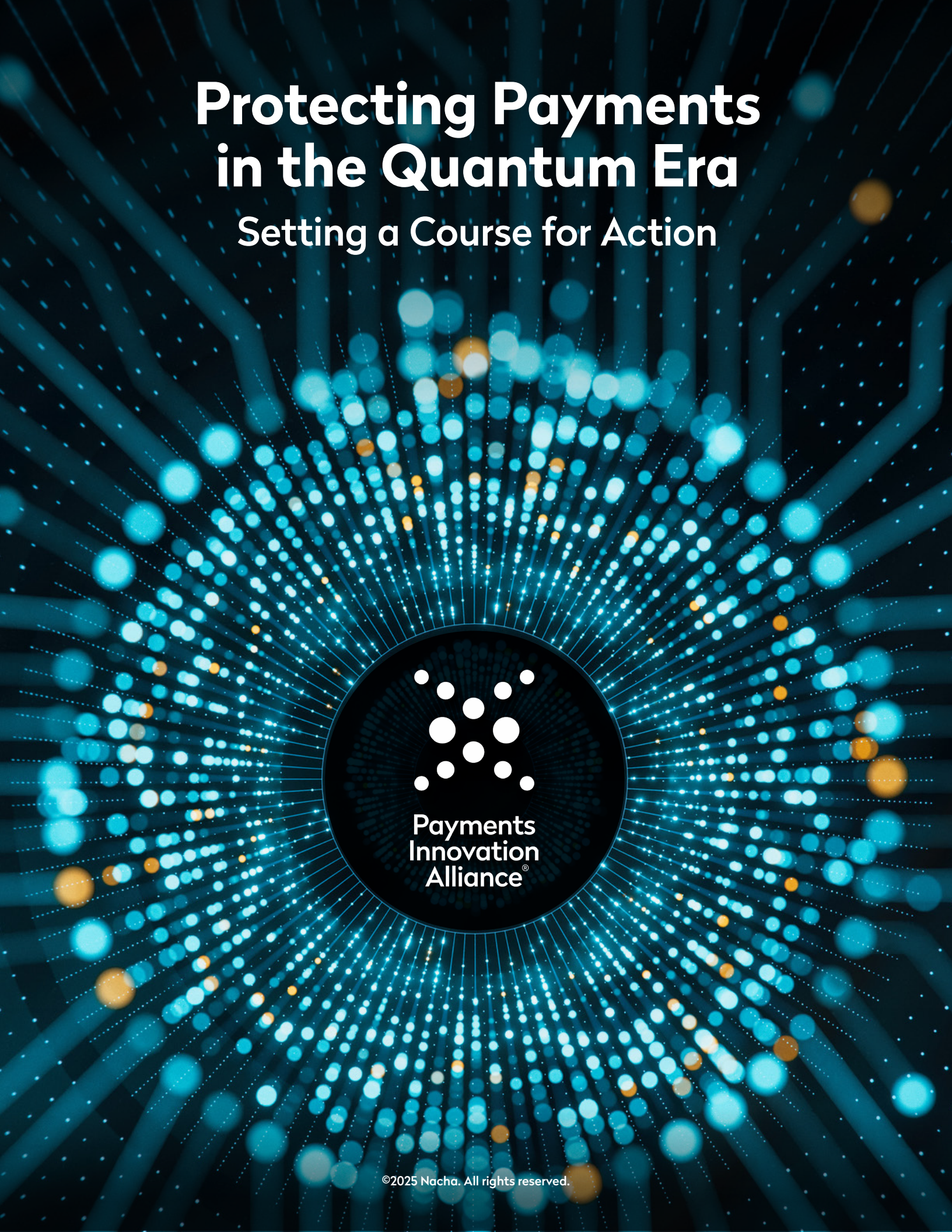
Protecting Payments in the Quantum Era

Setting a Course for Action



INTRODUCTION

Today's digital infrastructure and communications for payments rely heavily on cryptography to safeguard sensitive data. Quantum computing poses significant threats to the cryptographic foundations that currently secure electronic payment transactions from payment initiation through the receipt and storage of the data.

All organizations enabling encrypted communications and processing or storing data are impacted by the quantum security threat, including financial institutions (FIs), payment networks, third-party payment processors, and enablers.

Years to Quantum, also referred to as Y2Q, is the looming threat that quantum computers could decrypt today's widely used encryption methods, potentially disrupting critical systems and data security.

Because the weakest link in the payment networks puts all participants at risk, all stakeholders must take action to implement quantum-safe standards. This is a significant effort that is impossible to complete in a matter of months. Instead, it takes careful planning and a committed road map that is properly resourced.

This document aims to raise awareness about the risks posed by quantum computing and the necessary steps organizations need to take to ensure they are quantum ready. The high-level action plan helps payments participants chart a path forward to begin mitigating near- to long-term exposure posed by quantum computing.

Quantum Threats

Example 1

Fraudulent transactions

Bad actors can use quantum computing to generate new payment messages by creating false digital signatures and using them to generate a payment message as if it was generated by the FI's sender.

Quantum Threats

Example 2

Modification of payment

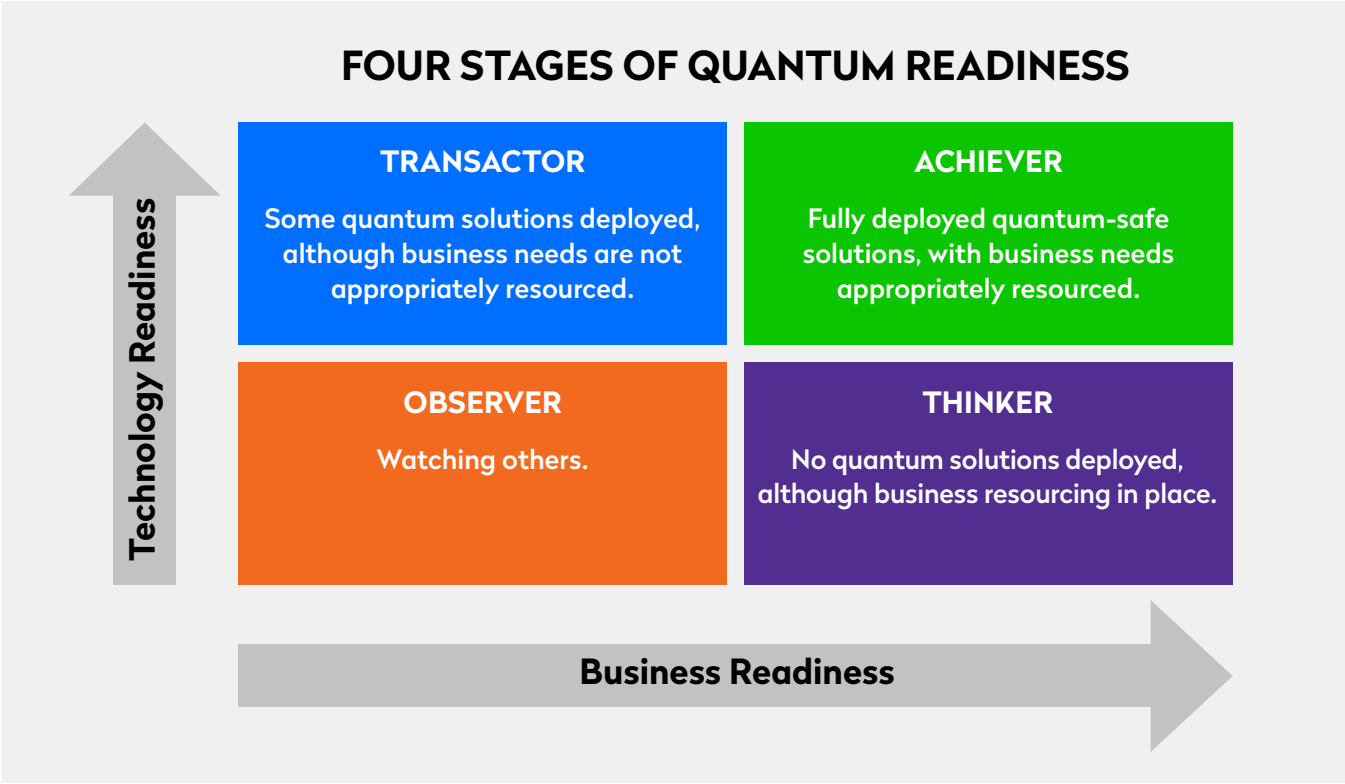
Bad actors can intercept the payment message and modify the payment instructions (e.g., beneficiary, amount). They may also modify or delete the stored payments data. FIs may have monetary losses, liquidity issues, and/or system outages as a result.

QUANTUM READINESS

The National Institute of Standards and Technology (NIST) Report on Post-Quantum Cryptography found that the first breaches might begin as soon as 2030.[1] However, the immediate threat to the payments ecosystem is "harvest now, decrypt later." Bad actors are busy now gathering encrypted data like account numbers and sensitive payments data they can easily decrypt and misuse once quantum computing is readily available to them.

Payments industry stakeholders will be exposed to potential regulatory penalties, monetary losses, and reputation risk and must act now to protect themselves from future threats. All devices and platforms used to transact payments data must implement quantum-safe encryption standards, including hardware and software, ATMs, smartphones, kiosks, point-of-sale devices, and more.

The following matrix can be used to assess the readiness stage for your overall organization and for each division. The end state is for your organization to embrace a strategy and initiatives that navigates from being an Observer to an Achiever.



Quantum readiness can be assessed based on the maturity of technology and business progress. There are four stages of readiness: Observer, Thinker, Transactor and Achiever.

1 https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf

ACTION PLAN FRAMEWORK AND RECOMMENDED ACTIONS

Technology and security leaders are critical to safeguarding the integrity of payment transactions and should be working now to ensure the resilience of their infrastructure in the quantum era. The following framework identifies the steps needed to support a quantum-safe future across the entire payments ecosystem.

AWARENESS AND EDUCATION

Quantum computing technology will fundamentally change the underlying security used. Stakeholders need to be aware of quantum computing developments and educate themselves on the impact of quantum computing from the viewpoints of technology, business, and organizational structure.

Recommended Actions

- ✓ **Quantum Leadership Team.** Form a Quantum Leadership Team that is accountable for making strategy and investment decisions, informing your Board of progress, and holding the organization responsible for future-proofing your assets and offerings.
- ✓ **Quantum Champion.** Designate a Quantum Champion responsible for developing the road map and driving the changes to make your organization quantum safe. They should be empowered to make decisions and/or engage with the leadership team to make these decisions.
- ✓ **Quantum Center of Excellence.** Create a Quantum Center of Excellence responsible for collaborating on solutions and understanding the internal and external impacts of changes. This cross section of subject matter experts may include representatives from cybersecurity, information security, technology, data stewards, compliance, product, operations, audit, and legal.
- ✓ **Research.** Understand what others are doing (e.g., NIST, regulators, third-party providers, cryptography providers supporting your payments infrastructure, etc.) to remain up to date on new developments and understand industry best practices.
- ✓ **Support and Training.** Build awareness and provide education at all levels, starting top down from the Board, to prepare for and address the benefits and risks of quantum computing.

STRATEGIC PLANNING

Develop a comprehensive quantum-safe strategy and road map that aligns with your timelines for technology upgrades, resource allocation, contingency planning, and funding.

Recommended Actions

- ✓ **Strategic Plan.** Your plan should be time-bound with assigned responsibilities.
- ✓ **Funding.** Secure funding to support your multi-year strategy, road map, and tactical plan.
- ✓ **Transparency.** Communicate and share the plan with your Board, internal stakeholders, and third parties.

IDENTIFY AND PRIORITIZE 'CROWN JEWELS'

Develop a comprehensive inventory of your most critical data and assets, considering technical and business perspectives. Assess your existing infrastructure to identify the magnitude of vulnerabilities that will inform your priorities.

Recommended Actions

✓ Inventory

Create a comprehensive inventory of systems, stored data, and third-party providers and enablers that currently rely on cryptography.

- Specify the type of cryptography being used: symmetric (single-key encryption) or asymmetric (public-key encryption).
- Assign one or more individuals to update the inventory going forward so you have a current view of what has or has not been remediated.

✓ Data

Identify and classify all data based on criticality for your operations, including customers' non-public personal information.

- Identify and classify data in transit and data at rest.
- Know where the data is stored, which may be at your organization and/or held by third parties (cloud, on premises, or hybrid).
- Prioritize the most sensitive data as the first area to apply quantum-safe solutions.

✓ Applications and Systems

Identify mission-critical systems and applications (the "crown jewels") that pose the greatest risk if your organization is breached by a quantum threat.

- Articulate the order in which systems and applications must be addressed, prioritizing mission-critical areas first.

✓ Policies and Procedures

Review and update data governance policies and procedures, including data retention policies and regulatory guidelines.

- Review and perform business continuity and disaster recovery plans.

Examples of Third-Party Providers and Enablers

- **Network service providers.**
- **Vendors supporting cryptography, certificates, public keys, tokens, multifactor authentication, digital signatures.**
- **Data storage providers – cloud, on premises, or hybrid.**
- **Payment and data processors – core and banking platforms.**
- **Fintech providers.**

RISK ASSESSMENT

Payment applications are categorized as critical because they generally operate 24/7/365. Most, if not all, payment stakeholders regularly perform risk assessments today. The quantum risk assessment – specific to your cryptographic infrastructure and that of your providers – can identify vulnerabilities that quantum computing could exploit.

Recommended Actions

- ✓ **Risk Management.** Create or update a risk management plan that incorporates the quantum threat.
- ✓ **External-Facing Applications.** Identify all existing external-facing applications and connectivity to your internal applications, (e.g., online banking or mobile banking) and create a plan for quantum-safe solutions.
- ✓ **Third-Party Processors and Enablers.** Work with your third-party processors and vendors, who enable or provide your current payment and cryptographic infrastructures, to plan for quantum-safe solutions.
- ✓ **Quantum-Safe Providers.** Identify and meet with providers who can help you implement quantum-safe solutions. Conduct a vendor risk assessment, according to your organization's policies and procedures, before choosing a partner.
- ✓ **Reporting.** Provide a risk assessment to your Board of Directors and senior leadership addressing the likelihood and impact of identified inherent risks and controls designed to mitigate risk to an acceptable residual level.

ADOPT QUANTUM-SAFE SOLUTIONS

Current cryptography will not withstand an attack from quantum computers. The threat to cryptography depends on sufficiently capable quantum computers and the ability to integrate quantum with other forms of hybrid or high-performance computing.

To address this vulnerability, NIST released three post-quantum encryption standards in August 2024.[2] The new standards are designed for two essential tasks:

- General encryption, used to protect information exchanged across a public network.
- Digital signatures, used for identity authentication.

Quantum-safe algorithms do not require using a quantum computer. These algorithms can be used with classical computing yet encapsulate mathematical computations to protect from cybersecurity attacks.

2 https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards
https://csrc.nist.gov/News/2024/postquantum-cryptography-fips-approved

The standards — containing the encryption algorithms' computer code, instructions for how to implement them, and their intended uses — are the result of an eight-year effort managed by NIST and involved participation from global expert cryptographers.

NIST encourages all cybersecurity experts and system administrators to start integrating the new post-quantum standards into their systems immediately because full integration will take time.

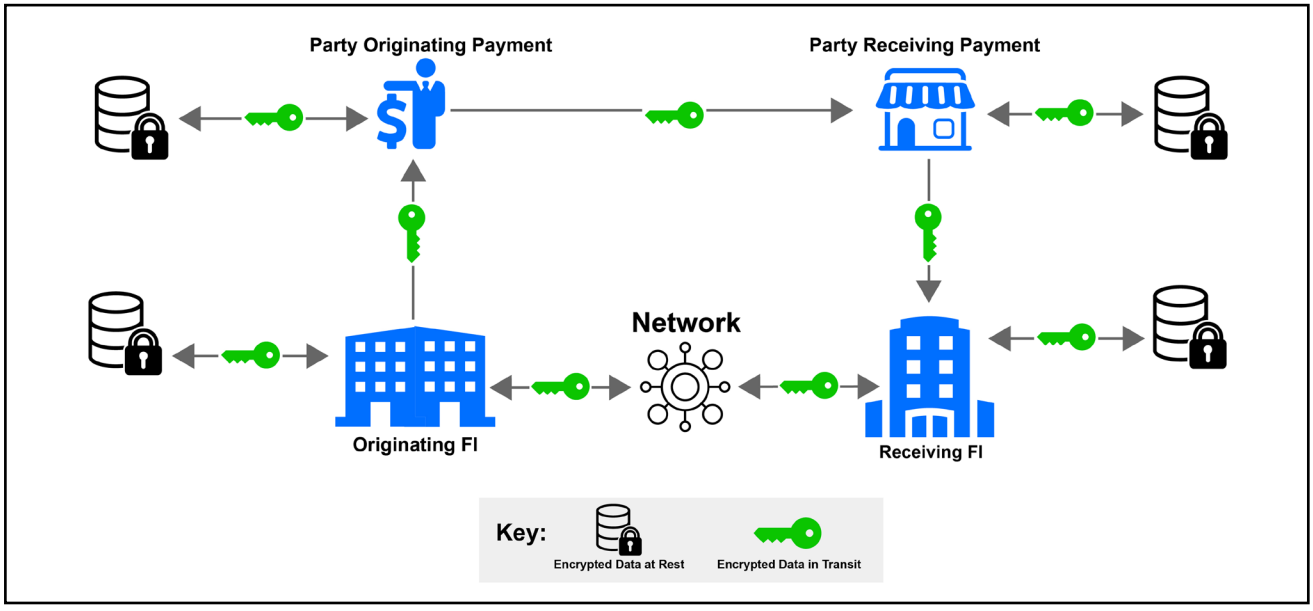
Recommended Actions

- ✓ **Data.** Start securing the most critical data first using the NIST post-quantum standards. The data may be held by you or a third party.
- ✓ **Proof of Concept.** Conduct a proof of concept (POC), evaluate results, and incorporate learnings. A POC can be done internally without the need to involve other parties.
- ✓ **Connectivity Among Payments Participants.** Today, all parties use some type of encryption or cryptography to secure data in transit and at rest. Reach out to the parties that enable your connections to understand their implementation road map and any implications for your business.

  Keep in mind these four key connectivity points:

  - Between a financial institution and the payment network.
  - Between a financial institution and its customers.
  - Between a financial institution and its third-party processors and vendors.
  - Within your organization's internal applications.

  Quantum-safe solutions between the networks and its participants should be accelerated because of the volume and value of payment transactions. Network providers need to consider the time to engage the entire ecosystem's education, testing, and implementation.



The diagram broadly illustrates the payments flow from an originating party to the receiving party. Any of the four key stakeholders may use multiple third parties. It is incumbent upon each stakeholder to implement end-to-end quantum-safe solutions for the hardware and software solutions it provides.

COLLABORATE AND INNOVATE

Your organization's quantum strategy can benefit from industry collaboration.

Recommended Actions

- ✓ **Join Industry Associations.** There are many industry associations you can join to network and share insights with peers, like Nacha's Payments Innovation Alliance. Assign your Quantum Champion to attend, engage, and report learnings back to your organization.
- ✓ **Engage your Cybersecurity Partners.** Work with your existing vendors (e.g., cloud providers, cybersecurity firms, hardware manufacturers, software providers) to validate when and how they will implement post-quantum cryptography.
- ✓ **Create a Knowledge Network.** Partner with government, academia, and other organizations to stay ahead of emerging quantum threats.
- ✓ **Work with Third-Party Providers.** Your third-party providers may offer educational forums to share their strategy and implementation plans.

JUMPSTART YOUR PLANNING

You need to rely on other organizations to update their cryptography to be quantum safe, and other organizations are relying on you to do the same. The following chart provides an illustrative high-level plan to help you get started on your multi-year, quantum-safe journey.

Period	Actions
0–1 year	• Form a Quantum Leadership Team and designate a Quantum Champion. • Conduct research on quantum computing. • Start collaborating with industry stakeholders. • Identify stakeholders who provide cryptographic solutions to understand their road maps. • Develop a multi-year strategic plan. • Create budget and fund initiatives that are aligned to the strategic and tactical plans.
1-2 years	• Conduct cryptographic inventory and risk assessment (e.g., current technology, capabilities, functionality, interrelationships, etc.) and identify critical priorities (i.e., "crown jewels"). • Identify key internal stakeholders, create a Center of Excellence and start training programs. • Start developing a Proof of Concept. • Reassess and reaffirm budget and funding.
2-3 years	• Assess Proof of Concept and adapt accordingly. • Implement quantum-safe solutions for all "crown jewels." • Identify any opportunities where quantum computing can be used. • Review and update organization policies, plans, and processes (e.g., information security, business recovery, etc.). • Adopt quantum-safe solutions for all new projects.
3-5 years	• Test and audit your systems for quantum threats. • Implement quantum-safe solutions for remaining assets and systems (i.e., beyond the "crown jewels").

CONCLUSION

The threat from quantum computing directly impacts the safety and soundness and very existence of the payments ecosystem. The weakest link exposes all participants; taking a proactive approach will help protect not only your organization, but the entire ecosystem. It is unpredictable when quantum computing will break today's cryptography, yet is likely to happen sooner than expected. The time to get started is now.

On June 7, 2024, the United Nations proclaimed 2025 as the International Year of Quantum Science and Technology (IYQ). According to the proclamation, this year-long, worldwide initiative will "be observed through activities at all levels aimed at increasing public awareness of the importance of quantum science and applications." [3]

The Payments Innovation Alliance is a membership program that shapes the future of the payments industry and develops thought leadership relevant to financial service institutions. This paper was developed by the Alliance's Quantum Payments Project Team which was established to create educational materials on quantum computing as it relates to the payments industry.

Visit the Quantum Payments Project Team page to learn more.

3 https://quantum2025.org/

Payments Innovation Alliance®