# The Impact of Quantum Computing on the Payment Card Industry

By the FS-ISAC Post Quantum Cryptography Working Group

# The Impact of Quantum Computing on the Payment Card Industry

## Contents



## Contributors


- Andrew Mulvenna
- Erwin Carrow, U.S. Bank
- Dr. Kenneth Giuliani, CIBC
- Oscar Covers, Dutch Banking Association
- Dr. Carrie Gates, FS-ISAC
- Mike Silverman, FS-ISAC


The opinions are those of the writers, are made as of the date of this document, and are subject to change without notice. Contributors' employers may have opinions that are different from and/or inconsistent with the views expressed in this document.

## Executive Summary

Quantum computing is a developing technology that uses principles of quantum mechanics to solve very difficult problems quickly. In the coming years, businesses in the payment card industry will be able to use this technology to conduct complex operations that are far too difficult for today's computers. That will expand the scope of their businesses enormously.

These capacities will be available to threat actors too. Experts predict quantum computers will be able to break all widely deployed classical public key cryptography (like RSA and elliptic curve cryptography) algorithms instantly, threatening the security of many technological systems throughout the financial sector. Over 20 billion devices will need to be migrated to quantum-safe cryptography.[i]

Leaders in the payment card industry (PCI) – and their suppliers – need to be prepared. To that end, the FS-ISAC Post Quantum Cryptography (PQC) Working Group – a global team of subject matter experts representing financial services, academia, and standard-setting entities – formed to advise the financial industry on quantum computing's challenges.

That's what we aim to achieve in this paper and its three companion documents. This document is designed for PCI technology leaders, and the companion documents offer guidance for practitioners. In all four publications, our focus covers:

### FS-ISAC PQC Working Group Publications

#### Business advisories

- Building Cryptographic Agility in the Financial Sector: Provides a framework for implementing crypto agility with insights on transition governance and architecture.
- Preparing for a Post-Quantum World by Managing Cryptographic Risk: Describes protocols that secure data against quantum and classical computers, with considerations regarding risk, data, regulations, and vendors.

#### Technical guidance

- Risk Model Technical Paper: Covers the current state of quantum computing, data, and resources to assess risk and prioritize remediation.
- Infrastructure Inventory Technical Paper: Lists assets to inventory, including encryption keys, algorithms, underlying technologies, and business processes.
- Future State Technical Paper: Defines quantum computing threats, and provides frameworks and risk assessment and readiness guidance.

- PCI cryptography that may be vulnerable to quantum, organized by use case and entity
- Discussion of key hardware and software components and the considerations that arise from quantum computing in the sector
- Use cases in the financial sector
- Potential concerns related to infrastructure and the life cycle of payment card processing
- Standards and quantum-specific cryptographic implementations related to payment cards

The threat to the PCI is not immediate, but it is urgent. Securing shared systems will require a collaborative effort to address collective impact. Through these publications, we hope to support the achievement of a quantum-safe environment for the financial services industry.

**Three companion documents provide a technological examination of specific use cases.**

- Use Cases 1 and 2: Card Provisioning Setup and Cardholder Data Provisioning
- Use Cases 3 and 4: Transaction Routing and Authorization and Retail Transaction Detail and Routing
- Use Cases 5 and 6: ATM and POS Card Capture and ATM and POS Setup With Backend Acquiring Systems

## The Impact of Quantum Computing on Cryptography

Payment cards are used for billions of transactions every day – 1.98 billion of them on credit cards alone – making payment cards an essential aspect of consumers' financial lives and the global economy.[ii]

It's clearly necessary to safeguard those transactions from serious risks like quantum computing, which will undermine important cryptography that those billions of


 

transactions depend on. Moving the cryptographic infrastructure from its current algorithms to crypto-resilient algorithms is a significant piece of work and will require the participation of multiple stakeholders across the card payment infrastructure.

The Payment Card Industry Security Standards Council (PCI SSC)[iii] does not mandate the type of cryptography that must be used for PCI use cases. PCI SSC guidance recommends using strong cryptography that is resistant to known attacks. This includes algorithms approved by the National Institute of Standards and Technology (NIST) for FIPS 140-2 certification.[iv] In addition, we note the NIST IR 8547 initial public draft, Transition to Post-Quantum Cryptography Standards.[v]

Until recently, technologists were advised to migrate to AES 256 due to the "key-halving" property of Grover's Algorithm. Current guidance from NIST advises AES 128-bit as sufficient to mitigate the threat of quantum computing. Depending on the use case, a 128-, 192-, or 256-bit key size is recommended.

Below are some of the current cryptographic algorithms that are commonly used for PCI card manufacturing.

| Encryption Type | Algorithm | Description |
|---|---|---|
| Symmetric | Triple-DES (3DES) | Most implementations are two-key Triple-DES |
| Symmetric | Advanced Encryption Standard (AES) | Though available, not in use in many cases |
| Asymmetric | RSA 2048 | In use for multiple use cases such as EMV (Europay, MasterCard, and Visa) cards and remote key loading |
| Asymmetric | Elliptic Curve Cryptography (ECC) | Available with the latest EMV specifications |

None of the asymmetric algorithms above are quantum resilient – i.e., resistant to cryptanalytics attacks from both traditional and quantum computers – and should not be


 

considered as part of a migration to a PQC-safe system. In addition, Triple-DES has been deprecated as an approved algorithm at the time of this writing.

Any migration should look at conversion to AES for the symmetric case. For the asymmetric case, PQC algorithms are recommended, which researchers have been working on and are resistant to attacks by quantum computers.

With regards to AES, the recommendation has been to migrate to AES 256 due to the "key-halving" property of Grover's Algorithm (a quantum algorithm for unstructured search that finds the unique input to a black box function that produces a particular output value).[vi] Recent guidance from NIST states that AES 128 would be sufficient to mitigate the threat of quantum computing.[vii]

## PCI Cryptography Use Cases Vulnerable to Quantum Computing

However, to migrate to new algorithms, users need to know where vulnerable algorithms exist.

The following table lists PCI cryptography that may be vulnerable to quantum, organized by use case and entity. The numbering system relates to our examination of the Banking Industry Architecture Network's (BIAN)[viii] level three and level four use cases and a fifth level we added to the BIAN model to more granularly describe the vulnerable business processes. That work is described in the Financial Use Cases section.

As with most threats, basic cybersecurity hygiene is fundamental to protection. Examples of good security practices are listed in Appendix A.


 

| Use Case Name (FS-ISAC PQC Working Group L5 of the Banking Industry Architecture Network) | | |
|---|---|---|
| 1 | Card provisioning setup (e.g. physical systems, HSMs, DBs, etc.) | Issuer |
| 2 | Cardholder data provisioning (PAN creation, creation of data for chip, mag-stripe, CNP, PIN, cardholder record storage) | Issuer, card personalization bureau |
| 3 | Card-present transaction routing and authorization (includes PIN routing and verification, chip transaction authorization, magstripe authorization, CNP verification, etc.) | Issuer, acquirer, merchant, card brand |
| 4 | Card-not-present transaction detail and routing | All |
| 5 | ATM and POS setup with backend acquiring systems (e.g. key injection) | Acquirer |
| 6 | ATM and POS card capture (i.e. actions taken when ATM and POS process transaction) | Acquirer |

The technology and architecture for these use cases vary between organizations and industries and by regulatory requirements. Note that implementing a secure and compliant system often involves a combination of hardware, software, and operational controls tailored to the specific needs and risks of the organization. Quantum computing will create unique vulnerabilities to algorithms and architectures in:

The numbering system of our fifth-level use cases also pertains to these sections:

- Standard-Setting Organizations
- Financial Sector Use Case

- Physical systems: PCI card use cases may involve physical systems such as servers, workstations, and other hardware components. These systems are responsible for managing the provisioning process and interacting with the necessary software and devices.

- **Hardware Security Modules (HSMs):** HSMs are specialized, tamper-resistant devices that provide secure key management, cryptographic operations, and protection of sensitive data. They ensure the confidentiality and integrity of cryptographic keys and perform secure operations, such as encryption and decryption, that are necessary for protection.

HSMs play a crucial role in securing sensitive information during several card processes.

- **Mobile devices**: While mobile devices were traditionally used for telecommunications, they now have many of the capabilities and functionalities of a credit or debit card, such as contactless transactions at point of sale (POS) devices.

- **Compliance with PCI standards:** The entire PCI card system must comply with the different requirements of PCI standards including PCI DSS and PCI PIN. This includes implementing appropriate security controls, regular vulnerability assessments, and compliance audits to ensure the protection of cardholder data and meet the standards set by the payment card industry.

- **Databases:** Databases are an essential component of many PCI card-related systems. They are used to store and manage cardholder data, including customer information, card details, and provisioning- and transaction-related data.

Databases need to be secured and comply with PCI DSS requirements to protect sensitive information.

- **Software:** Software facilitates the management and execution of many card processes. Software interacts with HSMs and databases to ensure secure and accurate operations.

- **Secure communication channels:** PCI operations require secure communication channels to transmit sensitive information safely between different system

components. Encryption protocols, secure APIs, or other secure communication mechanisms are used to protect data in transit and prevent unauthorized access or interception during provisioning operations.

## Financial Use Cases

The PQC Working Group thoroughly investigated the quantum threat using BIAN as our basis for the examination.

BIAN lists use cases down to four distinct levels of specification. As our purposes are more in-depth, we apply a fifth level to the BIAN model to describe the business processes made vulnerable in closer detail. Out-of-scope use cases are listed in Appendix B.

The following lists BIAN level three and level four, along with our fifth, more descriptive level.

| BIAN L3 | BIAN L4 | Description | FS-ISAC PQC Working Group L5 |
|---|---|---|---|
| Cards | Debit/Credit/Charge Card Fulfillment | The lifecycle of fulfilling a card, from creating numbers, setting interest rates and limits, etc. | Product definition (e.g., type of card, terms and conditions, interest rates) |
| | | | Card provisioning setup (e.g. physical systems, HSMs, DBs, etc.) |
| | | | Client request mechanism (i.e. tech channel through which requests are made) |
| | | | Initial account creation (backend, includes account number) |
| | | | Cardholder data provisioning and manufacturing (PAN creation, creation of data for chip, magstripe, CNP, PIN, cardholder record storage) |


 

| | | | |
|---|---|---|---|
| | | | Card activation (client activates card) |
| Cards | Card Authorizations | The authorization, settlement, and funding between merchants, their bank, the issuing bank, and the cardholder's account | Card-present transaction routing and authorization (includes PIN routing and verification, chip transaction authorization, magstripe authorization, IVR, etc.) |
| | | | Card status authorization (e.g. account in good standing, sufficient funds, account not deemed as fraudulent or lost/stolen) |
| | | | Transaction status authorization (e.g. transaction deemed anomalous or outside of usual client behavior, AI ML, AML, etc.) |
| | | | Settlement of accounts between merchant, acquirer, issuer |
| Cards | Card Capture | Capturing the payment at the point of sale or transaction, as well as card-not-present cases | ATM and POS setup with backend acquiring systems (e.g. key injection) |
| | | | ATM and POS card capture (i.e. actions taken when ATM and POS process transactions) |
| | | | Card-not-present transaction detail and routing |
| Cards | Card Billing and Payments | Bank to consumer issuing of bills and collecting payments | Transaction aggregation and sorting |
| | | | Bill creation |


 

| | | | |
|---|---|---|---|
| | | | Client payment through different channels |
| | | | Account updates based on client activity |
| | | | Delinquent account management |
| Cards | Merchant Relations | Establishing relationships, terms, and overall operations between the merchant bank and the merchant itself with the various networks | Business agreement between merchant and acquirer |
| | | | Resolution of fraudulent transactions |

It is important to note that while quantum computing vulnerabilities and exploits are a concern, practical quantum computers that can break current cryptographic algorithms are not yet available. By preparing in time for migration to quantum-safe encryption algorithms, costs can be significantly reduced. When quantum computers are available, certain use cases will require more attention than others.

## Quantum Computing Risks to Common Infrastructure Areas

From a technological perspective, the PCI business process use cases have the same characteristics as ubiquitous systems in any industry, as they make use of the same cryptographic protocols and technologies.

For embedded systems, there is still very little experience in securely implementing PQC algorithms in high assurance hardware environments. Therefore, it is advisable to gain experience with this as soon as possible.

This particularly concerns the implementation of PQC algorithms in POI/HSM firmware that must be resistant to side channel attacks as required in PCI PTS.


 

For software implementations, the effects of quantum will be limited to cryptography in common infrastructure. Examples of typical cryptographic methods for general use cases include:

- Transport Layer Security (TLS): TLS is commonly used to establish a secure connection between many business-to-business and business-to-consumer applications, including online banking, to ensure that the communication is encrypted during transit. TLS helps prevent eavesdropping and tampering with the message content.
- End-to-End Encryption: This method encrypts content on the sender's device and keeps it encrypted until it reaches the recipient's device. Only the sender and recipient have access to the decryption keys, ensuring that no one else can intercept and read the transmission.
- Pretty Good Privacy (PGP): PGP is a widely used encryption protocol that provides end-to-end encryption for email communication. It uses public-key cryptography to encrypt and decrypt messages, ensuring that only the intended recipient can read the message.
- S/MIME (Secure/Multipurpose Internet Mail Extensions): S/MIME is a protocol that adds digital signatures and encryption to email messages. It uses public-key cryptography to ensure the authenticity and integrity of the message and can also provide confidentiality through encryption.
- Internet Protocol Security (IPSec): A protocol at the packet level that authenticates and encrypts messages traversing a network at the network layer.

Systems implementing these technologies have been considered in the FS-ISAC report, Preparing for a Post-Quantum World by Managing Cryptographic Risk. This document, however, focuses on use cases that have unique and specific cryptographic implementations related to payment cards.

## Standard-Setting Organizations

Standard-setting organizations develop, coordinate, and amend standards relevant to financial services institutions' cybersecurity, such as technical, interoperability, and performance issues, among others. Meeting standards set by these organizations


 

isn't legally mandated, but many standards are integrated into regulatory frameworks that govern financial services sector operations.

**Examples of Standards and Standard-Setting Organizations in the Financial Services Sector**

- PCI DSS/PCI Security Standards Council: Policies and procedures that secure transactions and cardholders' data.[ix]
- ISO 20022/International Standardization Organization: Sets XML as the primary format for payment messages.[x]
- Security Controls Framework/Swift: Baseline controls for security measures.[xi]

The impact of quantum computing on the payment card industry will be affected by the actions of standard-setting bodies. Below are use cases, organizations, and considerations related to the standards that may be necessary for PCI cybersecurity in a post-quantum world.

| Use Cases | Organization | Consideration | Description |
|---|---|---|---|
| 1. Card provisioning setup<br>2. Cardholder data provisioning<br>3. Card-present transaction routing and authorization<br>4. Card-not-present transaction detail and routing<br>5. ATM and POS setup with backend acquiring systems<br>6. ATM and POS card capture | NIST | Approval and validation of PQC algorithms | Approval and validation of PQC algorithms |
| 1. Cardholder data provisioning<br>2. Card-present transaction routing and authorization | EMV Companies | Updating chip transactions and scripting standard | Change key derivation and transaction and script messaging to leverage AES |


 

| | | | |
|---|---|---|---|
| 3. Cardholder data provisioning<br>4. Card-present transaction routing and authorization | | Updating chip card verification and offline PIN encryption standard | Change the use of certificate structure to accommodate PQC or formulate a different approach |
| 1. Cardholder data provisioning<br>2. Card-present transaction routing and authorization | Card Brand - Regulation | Deciding on magnetic stripe authorization | Decide if risk with Triple-DES-based CVV is acceptable, change the formula for CVV to be AES-based, or decommission the magnetic stripe |
| 1. Card-not-present transaction detail and routing | | Deciding on card-not-present (CNP) authorization | Decide if risk with Triple-DES-based CVV2 is acceptable, change the formula for CVV to be AES-based, or determine another paradigm for CNP transactions |
| 1. ATM and POS card capture | ANSI/ISO | Definition of PIN block format | Definition of ISO PIN block 4 format (completed) |
| 1. ATM and POS setup with backend acquiring systems<br>2. ATM and POS card capture | | Amending DUKPT standard | Amend the DUKPT standard to support AES |
| 1. ATM and POS setup with backend acquiring systems<br>2. ATM and POS card capture | PCI SSC | Guidance on remote key loading | Update to standards for AES and PQC migration of RKL for both ATMs/EPPs and POS devices |


 

| | | | |
|---|---|---|---|
| 3. Card provisioning setup<br>4. ATM and POS setup with backend acquiring systems<br>5. ATM and POS card capture | | Timelines for key exchange and PIN conveyance | Publication of timelines for migration ANSI PIN Block 4 (using AES) and TR-31 |
| 1. Card provisioning setup<br>2. Cardholder data provisioning<br>3. Card-present transaction routing and authorization | Global Platform | Strategy for Secure Element (SE) and Trusted Execution Environment (TEE) functions standard (asymmetric key) | Determine a strategy to enable this capability |
| 1. Card provisioning setup<br>2. Cardholder data provisioning<br>3. Card-present transaction routing and authorization | | Timelines for SE and TEE functions standard (symmetric key) | Establish a timeline for migration to AES from Triple-DES |

## Organizational Implementation: Roles and Considerations

Many of the aspects of quantum vulnerability – such as keys – are related to technologies built by hardware and software manufacturers and providers. There are also traditional risks that hardware manufacturers in particular need to consider when it comes to implementing PQC encryption algorithms in firmware for high assurance environments. As such, these organizations will be involved in implementing the migration to quantum safety. Below are proposed use cases and considerations related to the transition.

| Use Cases | Organization | Consideration | Description |
|---|---|---|---|
| 1. Card provisioning setup<br>2. Cardholder data provisioning<br>3. Card-present transaction routing and authorization<br>4. Card-not-present transaction detail and routing<br>5. ATM and POS setup with backend acquiring systems<br>6. ATM and POS card capture | HSM Manufacturer | Implementing new key and PIN specifications | Support for AES keys and PQC asymmetric algorithms as dictated by new standards. Specific consideration may need to be given to the implementation of PQC algorithms that must be resistant to side channel attacks |
| 1. Card-present transaction routing and authorization<br>2. ATM and POS setup with backend acquiring systems<br>3. ATM and POS card capture | EPP and PED Manufacturer | Implementing new PIN algorithms and RKL specifications | Support for AES keys and PQC asymmetric algorithms. Specific consideration may need to be given to the implementation of PQC algorithms that must be resistant to side channel attacks as required in PCI PTS. Also consideration may need to be given to the distribution of AES keys prior to the availability of PQC algorithms and hardware |


 

| | | | |
|---|---|---|---|
| 1. ATM and POS setup with backend acquiring systems<br>2. ATM and POS card capture | Chip Manufacturer | Implementing new EMV specifications | Production of EMV chips to support AES and PQC algorithms. Specific consideration may need to be given to the implementation of PQC algorithms that must be resistant to side channel attacks |
| 1. Card provisioning setup<br>2. Cardholder data provisioning<br>3. Card-present transaction routing and authorization | Mobile Device Manufacturers | Implementing new EMV and global platform specifications | Production of mobile devices to support AES and PQC algorithms |
| 1. ATM and POS card capture | Card Brands - Processing | Migration of interchange transaction routing | Migration to AES keys. This is to be done in coordination with issuers and acquirers |
| 1. Card-present transaction routing and authorization<br>2. Card-not-present transaction detail and routing<br>3. ATM and POS card capture | | Migration of Stand-In Processing (STIP) | Migration of STIP services for EMV, magnetic stripe, CNP, and PIN verification |
| 1. ATM and POS card capture | Acquirer/Payment Service Provider (PSP) | Migration of interchange transaction routing | Migration of ZMK and interchange keys to AES. This is to be done in collaboration with card brands |


 

| | | | |
|---|---|---|---|
| 2. ATM and POS setup with backend acquiring systems<br>3. ATM and POS card capture | | Migration of EPP and POS systems to new PIN capabilities and RKL | Migration of EPP and POS PEDs to support AES and PQC algorithms. Migration of backend systems |
| 1. Card provisioning setup<br>2. Cardholder data provisioning | Issuer | Migration of card production systems | Migration of PIN production to AES. Migration to AES and PQC in EMV. Migration to changes in magnetic stripe and CNP |
| 1. Card-present transaction routing and authorization | | Migration of interchange transaction routing | Migration of ZMK and interchange keys to AES. This is to be done in collaboration with card brands |
| 1. Card-present transaction routing and authorization<br>2. Card-not-present transaction detail and routing | | Migration of transaction authorization systems | Migration of backend authorization systems to AES and PQC in EMV. Migration to changes in magnetic stripe and CNP. Migration to new PIN verification methods |
| 1. Cardholder data provisioning<br>2. Card-present transaction routing and authorization | | PIN storage migration | Migration to AES for PIN storage |


 

| | | | |
|---|---|---|---|
| 1. Card provisioning setup<br>2. Cardholder data provisioning | Card Embossers | Migration of PIN mailing systems | Migration PIN mailer systems to leverage AES in PIN storage and conveyance |
| 1. Card provisioning setup<br>2. Cardholder data provisioning | | Migration of card-related functions | Migration to chips leveraging new EMV and PIN specifications. Migration to changes for magnetic stripe and CNP data |

# Appendices

## Appendix A: Best Practices

As with most threats, protection begins with good cybersecurity hygiene. The following best practices and guidelines protect cardholder data and prevent vulnerabilities.

- Implementing strong access controls: Restrict access to systems and networks that store or process cardholder data. Only authorized personnel should have access to these systems.
- Encrypting sensitive data: Encrypt cardholder data during transmission and storage. Use strong encryption algorithms and secure key management practices.
- Regularly updating and patching systems: Keep all systems and software up to date with the latest security patches and updates. This helps address any known vulnerabilities and protect against potential exploits.
- Implementing secure coding practices: Develop secure software applications and systems that handle cardholder data. Follow secure coding guidelines and conduct regular security assessments and code reviews.
- Regular monitoring and auditing: Implement robust monitoring and auditing processes to detect and respond to any unauthorized access attempts or suspicious activities.


 

- Risk assessment: Identify the assets that are at risk from quantum computing attacks and assess the likelihood and impact of such attacks.
- Mitigation strategies: Implement the appropriate mitigation techniques to reduce the risk of quantum computing attacks.
- Detection and response: Implement measures to detect and respond to post-quantum computing attacks if they do occur.

## Appendix B: Out-of-Scope Financial Use Cases

As described in the Financial Industry Use Cases table, certain use cases in the BIAN model leverage general cryptographic protocols that are not in scope for this document. This section details why these use cases are not under discussion.

| Use Case | Reason Not Relevant/Not Applicable |
|---|---|
| **Product definition** | This use case involves business strategic decision-making in the card space based on analysis of client base, market conditions, and business opportunity. Typically, the technological systems involved are only used for storage and data transfer. This is usually handled by existing systems. |
| **Client request mechanism** | This involves the channel of request – such as online, in-person, phone, or mail – or modification of a card product. While there may be personally identifiable information (PII) involved in the client request on a dedicated channel, there is nothing card-specific in client requests, and the mechanisms in place are considered standard infrastructure. |
| **Initial account creation** | This use case involves the creation of the client account, including the account number (not PAN), and preparing the issuer's backend system for future cards to be issued. While there is PII involved, this is just an account setup similar to account setup in any other client-facing business use case. Thus, standard infrastructure would be present here. |
| **Card activation** | This is the process of client with card in hand activating their card for use. The card itself is not materially changed during this event. |

| | |
|---|---|
| | This is merely a communication through a designated channel to the issuer's backend system notifying it to be ready for transactions. This state change on the backend system qualifies as a standard generic account update and so uses standard infrastructure. |
| **Card status authorization** | During the transaction, the card is looked up in the issuer's book of record to determine if the card is listed as valid, has been activated, and has not been canceled or suspended. This amounts to a general lookup through communication channels using standard infrastructure. |
| **Transaction status authorization** | This use case involves fraud analysis on a particular transaction. Issuer fraud systems would look at the metadata surrounding a transaction to determine if the transaction is in line with a client's usual behavior or is to be deemed anomalous. It would also include possible extra authentication such as an SMS message. Typically, this use case involves intelligence and decision-making based on available data and could potentially leverage AI and ML. However, this would be akin to other real-time fraud detection systems in other use cases and so use standard infrastructure. |
| **Settlement of accounts** | This use case deals with the settlement of accounts between issuer, acquirer, merchant, and card brand. This typically involves the transmission of substantial amounts of data between backend systems. While each type of transmission has its own format, it is just the transfer, update, and aggregation of data that is normally handled by standard infrastructure. |
| **Transaction aggregation and sorting** | This use case is no different from standard aggregation and sorting of any large dataset. While there may be cryptographic-related technologies involved in things such as PAN protection (e.g. tokenization), these will be considered in a separate use case. This one is standard data manipulation using standard infrastructure. |
| **Bill creation** | This use case involves the processing of individual account data into standard format for a bill and proper presentation and |

| | |
|---|---|
| | notification that the bill is ready. This involves data processing, alerting, and visual display using standard technologies. |
| **Client payment through different channels** | This use case deals with the method of payment of a credit card bill. This falls into the payment space but is not card-based. It uses quantum-vulnerable technologies but is not card-specific. |
| **Account updates based on client activity** | This use case involves updating a client's account when any modification takes place, such as a change of address, balance, rewards points, or any other such activity. It amounts to a standard input mechanism as well as a backend data update. |
| **Delinquent account management** | The resolution of delinquent accounts can involve messaging, drafting of letters, consultation, payment plan development, and even legal action. There are various technical and non-technical processes, all of which use standard technology. |
| **Business agreement between merchant and acquirer** | This involves consultation and legal agreements between merchant and acquirer. This is not a dedicated system and would use standard technology. |
| **Resolution of fraudulent transactions** | This use case could involve consultations between client, issuer, and merchant as well as investigations into the validity of the fraud leading to resolution. This mostly occurs outside the technological realm and involves little more than communication and account updates using standard technology. |

## References and Resources

[i]World Economic Forum, 2022. *Device migration to quantum-safe cryptography*. [pdf] Available at: https://www3.weforum.org/docs/WEF_Transitioning%20to_a_Quantum_Secure_Economy_2022.pdf
[ii]Federal Reserve, 2025. *Federal Reserve Payments Study*. [online] Available at: https://www.federalreserve.gov/paymentsystems/fr-payments-study.htm,
Capital One Shopping, 2025. *Number of Credit Card Transactions*. [online] Available at: https://capitaloneshopping.com/research/number-of-credit-card-transactions/


 

[iii]PCI Security Standards Council, 2025. *PCI DSS (Payment Card Industry Data Security Standard)*. [online] Available at: https://www.pcisecuritystandards.org/standards/pci-dss/
[iv]National Institute of Standards and Technology (NIST), 2025. *Cryptographic Module Validation Program: FIPS 140-2*. [online] Available at: https://csrc.nist.gov/Projects/cryptographic-module-validation-program/fips-140-2
[v] National Institute of Standards and Technology (NIST), 2024. *NIST IR 8547: Initial Public Draft*. [pdf] Available at: https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8547.ipd.pdf
[vi]Guo, C., 2023. *Grover's Algorithm - Implementations and Implications*. [online] Available at: https://www.researchgate.net/publication/369470958_Grover's_Algorithm_-_Implementations_and_Implications
[vii]National Institute of Standards and Technology (NIST), 2025. *Post-Quantum Cryptography FAQs*. [online] Available at: https://csrc.nist.gov/projects/post-quantum-cryptography/faqs#:~:text=Based%20on%20such%20understanding%2C%20current%20applications%20can,when%20we%20can%20foresee%20a%20transition%20need
[viii]Banking Industry Architecture Network (BIAN), 2025. *BIAN*. [online] Available at: https://bian.org/
[ix]PCI Security Standards Council, 2025. *PCI DSS (Payment Card Industry Data Security Standard)*. [online] Available at: https://www.pcisecuritystandards.org/document_library/?document=pci_dss
[x]ISO 20022, 2025. *ISO 20022*. [online] Available at: https://www.iso20022.org/
[xi]Swift, 2025. *Customer Security Programme (CSP) - Security Controls*. [online] Available at: https://www.swift.com/myswift/customer-security-programme-csp/security-controls


 