ENCRYPTION CONSULTING

CASE STUDY

COMPLIANCE SERVICE

Bringing a US bank up to PCI DSS 4.0 with a full encryption assessment

A leading US retail bank with over 15,000 employees needed to meet the stricter demands of PCI DSS 4.0. Our encryption assessment found the gaps across its multi-cloud and on-premises environments, and mapped the path to compliance.

SECTOR	SIZE	ENGAGEMENT
Retail banking (US)	15,000+ employees	PCI DSS 4.0 assessment

PCI 4.0
Compliance achieved

15,000+
Employees protected

TLS 1.2+
Protocols modernized

A leading US bank, scaled by digital innovation

Our client is a prominent US retail bank known for a broad range of financial services. With more than 15,000 employees and a nationwide network of branches and ATMs, it has been a trusted name in personal banking, credit cards, loans, and wealth management for millions of customers.

Over the past decade the bank has grown rapidly through digital innovation, from mobile banking apps to 24/7 support and online loan processing, setting new standards in customer service and operational excellence. With that growth came a large daily volume of transactions and sensitive cardholder data to protect.

For a bank processing cardholder data at scale, PCI DSS isn't just a standard to pass. It's the difference between earning customer trust and risking it.

Compounding gaps, under a stricter standard

An encryption assessment across the bank's multi-cloud and on-prem environments surfaced a stack of compounding gaps.

1

Outdated hashing

Cardholder data was stored with plain one-way hashing, no salting or keyed hashing, leaving it open to brute-force and precomputed attacks.

2

Obsolete protocols

Some systems still ran SSL and old TLS, relying on weak algorithms like MD5, RC4, and SHA-1 that invite man-in-the-middle attacks.

3

Co-located keys

Encryption keys lived in the same environment as the data they protected, so a single breach could expose both the keys and cardholder data.

4

Non-compliant vendors

Some payment processors and cloud providers fell short of PCI DSS, safeguarding cardholder data with inadequate encryption and access control.

5

Retained SAD and aging policies

Sensitive Authentication Data like CVV and PIN blocks wasn't reliably deleted after authorization, and weak password and MFA practices couldn't keep pace with the stricter PCI DSS 4.0 standard.

> The gaps weren't theoretical: outdated hashing, obsolete protocols, co-located keys, and non-compliant vendors created a compounding risk profile that PCI DSS 4.0 was specifically designed to eliminate.

ENGAGEMENT SUMMARY · ENCRYPTION CONSULTING · COMPLIANCE SERVICES

From assessment to remediation

We mapped the bank's cryptographic environment, ran a full gap analysis against PCI DSS 4.0, and delivered a prioritized remediation plan across hashing, keys, access, and vendors.

Assessment and gap analysis

We gathered policies, ran stakeholder workshops, mapped data flows end to end, and analyzed every control against PCI DSS 4.0.

Modern hashing and protocols

We recommended keyed HMAC hashing in place of plain one-way hashing, and upgrading SSL and old TLS to TLS 1.2 or higher.

Tokenization for card data

Vault-based tokenization replaces cardholder data with non-sensitive tokens, so a breached system reveals tokens, not real data.

Isolated keys in HSMs

A dedicated KMS keeps keys isolated from the data they protect, with HSMs ensuring keys are never exposed in plaintext.

MFA, FIDO, and RBAC

We advised MFA across the cardholder data environment, FIDO-based auth for high-risk access, tighter RBAC, and stronger password policies.

Vendor and data governance

We enforced PCI compliance on third-party vendors through audits and contracts, and set SAD to auto-delete or mask after authorization.

Compliant, and far harder to breach

The remediation plan closed the gaps and modernized the bank's cryptography, cutting breach risk while bringing it fully in line with PCI DSS 4.0.

58%

Lower data breach risk after remediation

Stronger data protection

TLS 1.2 or higher, tokenization, and keyed hashing now protect cardholder data both at rest and in transit.

PCI DSS 4.0 compliant

The bank aligned with the latest standard, cutting the risk of penalties and breach-related fallout.

Vendors under control

Regular risk assessments, audits, and contractual requirements brought third-party vendors into compliance.

Efficient, ongoing compliance

Automated SAD deletion and account lockouts cut manual work, while regular audits keep compliance on track over time.

IN SUMMARY

A compliant base, built on customer trust

In financial services, trust is everything. Our PCI DSS 4.0 assessment gave the bank a clear, actionable picture of its security gaps and a practical remediation plan to close them. From keyed hashing and TLS 1.2+ to vault-based tokenization, isolated keys in HSMs, stronger MFA and RBAC, and tighter vendor governance, the bank modernized its cryptographic foundation and cut data breach risk by 58%. It now meets PCI DSS 4.0, protects cardholder data far more effectively, and is set up to maintain compliance, and customer trust, as it grows.

GET STARTED

Assess your PCI DSS compliance.

Talk to our Compliance team →