FinWise Bank Data Breach: When Encryption Is the Only Defense Left

Administrator | 26/10/2025 | CYBERSECURITY

A breach that came from inside

It wasn’t a hacker from abroad.
It was someone who used to work there.

On **May 31 2024**, a **former FinWise Bank employee** accessed internal systems using credentials that were never revoked.
He leaked personal information belonging to **689 000 American First Finance customers**.
The worst part? The breach went **undetected for more than a year** — until **June 18 2025**.

This case shows how **insider threats** can quietly bypass even the most expensive cybersecurity tools when basic access controls fail.

What really went wrong

According to lawsuits, the stolen data **wasn’t properly encrypted**.
That single flaw turned a contained incident into a catastrophic leak.

If encryption had been enforced end-to-end — and if keys were kept apart from the databases — the exposed records would have been unreadable.
Instead, FinWise now faces **class actions**, **regulatory scrutiny**, and a **massive reputational loss**.

Experts say this breach highlights a blind spot many banks share: **security governance**.
They focus on blocking external attackers while overlooking **former staff, contractors, and privileged insiders** who already know the system.

© 2026 - All rights reserved. Project Osint – OSINT, AI & Cybersecurity | projectosint.com

Encryption isn’t a checkbox — it’s survival

Encryption is often described as the *last line of defense*.
In reality, it’s the **foundation of digital trust**.

When properly applied, encryption ensures that even if criminals gain access, **data remains useless without the decryption keys**.
But encryption alone isn’t enough.
What protects the keys themselves matters even more.

Key management: where most institutions fail

A strong **Key Management System (KMS)** stores encryption keys in a **separate, isolated environment**.
This segregation means even administrators who manage databases **cannot access the keys** that unlock them.

Had FinWise implemented such separation, the ex-employee could have stolen data — but **not decrypted it**.
That single architectural choice would have turned a data breach into an empty theft.

From encryption to full visibility

Modern data protection demands visibility as much as cryptography.
Financial institutions need to know **who accesses what, and when**.

Centralized control platforms like **D.AMO Control Center** — developed by Penta Security — allow real-time monitoring of access logs, privilege changes, and abnormal activity.
This kind of oversight could have revealed the FinWise intrusion months earlier.

The broader message: **encryption without monitoring is like a safe without a guard**.

When detection comes too late

© 2026 - All rights reserved. Project Osint – OSINT, AI & Cybersecurity | projectosint.com

Every day a breach goes unnoticed multiplies its cost.
FinWise discovered the intrusion more than twelve months later — an eternity in cyber-time.

The delay exposed customers to identity theft, regulatory penalties, and lasting distrust.
In banking, where confidence is currency, **transparency and rapid disclosure** are as vital as encryption itself.

Building proactive defenses

The FinWise case offers a clear checklist for institutions handling sensitive data:

1. **Encrypt everything** — databases, backups, and endpoints.
2. **Separate encryption keys** with an independent KMS.
3. **Monitor privileged accounts** and audit every login.
4. **Revoke credentials** immediately after employment ends.
5. **Simulate insider attacks** to test resilience.

Solutions such as **Penta Security's D.AMO suite** integrate these layers: encryption, KMS, and centralized control.
They comply with standards like **GDPR**, **CCPA**, and **PCI-DSS**, helping banks move from *reactive response* to *proactive prevention*.

What the industry should learn

The FinWise breach isn't unique — it's a warning.
As digital banking expands, **the human factor** remains the weakest link.

© 2026 - All rights reserved. Project Osint – OSINT, AI & Cybersecurity | projectosint.com

Technology alone can’t guarantee security, but **encryption done right** can guarantee that stolen data stays meaningless.
The goal isn’t to stop every breach; it’s to ensure that, when one happens, **nothing valuable escapes**.

© 2026 - All rights reserved. Project Osint – OSINT, AI & Cybersecurity | projectosint.com