USE CASE

Real-World Insider Threats in the Financial Sector

Every day, financial institutions handle highly sensitive metadata—such as client identities, transaction histories, account balances, access logs, and internal communications. This makes the financial services sector one of the most frequently targeted industries, with firms reportedly facing cyberattacks up to 300 times more often than organizations in other sectors.

This use case examines key incidents within the sector to demonstrate how cybersecurity solutions can safeguard financial metadata, deter insider threats, and prevent data exfiltration.
By analyzing these incidents, organizations can uncover vulnerabilities, enhance security posture, and ensure ongoing compliance with regulatory standards.

INCIDENT REPORTS OVERVIEW

This section highlights two real-world insider breach cases in the financial sector, showing how sensitive client data was accessed and leaked, often due to weak internal controls.

01 Toronto-Dominion Bank (TD Bank) – New York

In December 2024, an insider data leak was discovered at TD Bank's New York office involving a newly hired anti-money laundering employee. The staff member used a personal mobile phone to secretly capture screen images of over 255 scanned client checks and personal details of nearly 70 customers. These images were then shared via Telegram, where they were made accessible to cybercriminal groups. The breach was detected when law enforcement launched an investigation following a series of fraud complaints, eventually uncovering forensic evidence on the employee's mobile device, including Telegram conversations and the captured check images.

02 USAA (via Teleperformance Call Center) – U.S. Staff

Between 2021 and 2024, a long-running insider scheme was carried out by employees at a U.S.-based Teleperformance call center serving USAA clients. Several call center agents conspired to leak sensitive client data and were eventually charged with conspiracy to commit bank fraud, as reported in December 2024. While the exact methods varied, investigators revealed that some staff likely used personal mobile phones to photograph on-screen data or copied it into private messaging apps. These actions enabled the sale or transfer of client information to fraud networks over time. The breach affected multiple resources, including USAA's remote support systems, Teleperformance CRM platforms, agent workstations, and unauthorized mobile apps.

COMPARATIVE ANALYSIS

Similarities

Both TD Bank and USAA incidents involved insiders accessing and leaking sensitive client data. In both cases, authorized users misused their access to confidential information, highlighting insider threats as a critical risk.

Differences in Impact

TD Bank's breach impacted 8 clients and was detected and handled quickly, including firing the employee and offering identity protection.
USAA's data breach happened through a third-party call center (Teleperformance) and lasted over a year. During that time, insiders used stolen customer data to create fake checks, resulting in over $2 million in fraud. The long delay in detection made the impact much worse.

Recurring Trends

- Weak internal monitoring allowed insiders to access and export sensitive data undetected.
- No visual deterrents like watermarks or session tagging were in place to discourage screen captures or alert admins.
- Long detection periods increased the scale of the damage.

COMPARATIVE ANALYSIS

To reduce the risk of insider threats and improve data protection across financial environments, organizations should consider the following steps:

Use Visible Deterrents

Applying on-screen watermarks that display user identity, time, and access details can discourage unauthorized screen captures and help trace any leaks.

Secure Document Printing

Adding dynamic watermarks to printed materials ensures sensitive information remains traceable even after leaving the digital environment.

Restrict Copy and Capture

Disabling clipboard access and screen capture tools is critical in preventing common data extraction methods.

Monitor Web-Based Access

For internal banking platforms or systems with source code access, displaying user identifiers on web sessions strengthens accountability and transparency.

Enhance Mobile Oversight

Financial data accessed on mobile devices—especially in remote or BYOD setups—should be closely monitored with safeguards that log and limit access.

Strengthen Access Controls

Implement role-based access and ensure third-party contractors only see what they need. Regular audits can catch risky access early.

Enable Real-Time Alerts

Track user actions with logging and behavioral alerts to detect suspicious activity quickly, especially across outsourced operations.

Ongoing Training

Regularly train both staff and third-party vendors on secure data handling practices, incident response, and the consequences of mishandling information.

By implementing these features, organizations can significantly reduce the risk of insider threats and unauthorized data access, ensuring better protection of sensitive information.

Conclusion

Financial institutions face high risks from insider threats due to the sensitive data they handle daily. The TD Bank and USAA incidents show how weak monitoring and lack of visible deterrents allow insiders to misuse data, causing serious harm.

Key lessons highlight the need for faster detection and stronger controls. Using tools like screen and print watermarking, restricting screen capture, monitoring web and mobile access, and enforcing role-based permissions can greatly reduce risks.

Combining these measures with ongoing training and real-time alerts helps organizations protect client data, prevent leaks, and respond quickly to threats—strengthening their overall security.