PKWARE Secures Bank Data After Breach Reveals Multiple Weaknesses

In 2014, one of the largest banks in the country suffered a data breach that compromised millions of customer records. The large-scale theft of unencrypted data resulted in significant SEC fines and a loss of shareholder and consumer confidence. In the aftermath of the event, the bank terminated its senior security team.

A Threat Within a Crisis

While still reeling from the data breach, the bank conducted an internal audit of its security practices and discovered another serious vulnerability. Many employees, the banks’ auditors found, were applying their own end-user encryption (using a variety of applications) to protect data in outbound emails. While encrypting sensitive data was a good idea in theory, in practice these employees were exposing the bank to further sanctions and data loss.

Pain Points

- Unprecedented Theft of Sensitive Customer Information
- Encryption Policies Fail Audit
- Potential for Additional Data Loss
- Exposure to New Fines and Sanctions

The Solution

1. Policy Applied Company-Wide
270,000 Desktop Installations in Less Than One Month
100% Compliance with Banking Disclosure Audit

Every Company’s Nightmare
The problem lay in the fact that the bank had no company-wide policy for data encryption. Emails protected by non-standard applications were not accessible by the bank’s data loss prevention (DLP) technology, so the DLP scanner could not identify emails in which employees sent data they were not authorized to share. Further, the lack of DLP visibility left the bank unable to comply with SEC and FINRA requirements related to data tracking and reporting.

**PKWARE’S SMARTCRYPT**

The bank’s new security team had several urgent objectives: restoring board and customer confidence, improving data protection and auditability, and ensuring compliance with government regulations.

In order to meet these demands, the bank’s Executive Director of Global Technology and Senior Security Architect selected PKWARE’s Smartcrypt as the corporate standard for file and email-based encryption. Smartcrypt’s persistent data-level protection and policy-based key management made it an ideal solution for the bank’s security needs.

By deploying Smartcrypt on 270,000 end-user desktops, the bank ensured that sensitive data would be protected in a way that the organization could control. Every desktop encryption operation now includes one or more public keys, allowing the bank’s DLP technology to decrypt and scan outgoing emails using a corresponding private key.

In addition to improving data security, Smartcrypt has helped the bank address its regulatory concerns. With full integration between Smartcrypt and its DLP scanner, the bank can conduct contextual data searches when subpoenaed for specific content, and is now in compliance with federal requirements that it maintain a copy of all decryption keys.

**LOOKING AHEAD**

Selecting Smartcrypt allowed the bank to move quickly and effectively at a time of intense internal and external scrutiny. The Smartcrypt implementation took only a matter of weeks, as it required no new infrastructure or changes to the bank’s existing security and network systems.

With minimal requirements for employee training and ongoing maintenance, Smartcrypt has enabled the bank to securely exchange sensitive information, exceed its compliance requirements, and restore customer confidence.