CASE STUDY

Preserving Client Trust

Discover and Protect Client Personal and Financial Data

Search Client Personal Data

- Servers, NAS, Email, cloud
- Office documents and archives
- PCI , Bank and SWIFT data

Key Business Benefits

- Proactively manage and secure
- Easy to deploy
- High accuracy reduces errors
- Compliance with PCI-DSS

Business Insights

- Centralized reports on PCI data
- Monitor PCI data protection
- Policy reinforcement

Safeguarding Client Information Fortifies Trust and Garners More Business

A commercial Bank that services the greater Bay area community and manages hundreds of millions of dollars in its 15-branch network needed to safeguard client information. As a community-based their banking experience is differentiated by offering more customized programs, local investments and presence in community outreach programs. They provide personalized money management in a trustworthy and reliable setting for their constituency.

Business Challenges

The Bank's advisors, associates, administrators and support staff are the faces of the Bay area community. Clients and business associates come to trust them for money management. They maintain a secure environment for their human resources teams that work with employee data, invest in trusted relationships with their HR outsourcing provider to keep employee data private. However, recent news of data breaches in the financial sector alarmed the Compliance team and prompted an initiative to review employee data privacy, and to establish practices of examining client data privacy. Their compliance team was keenly interested in an assessment to find insecure PII and PCI data across the branches and in headquarters, including:

- Social security numbers
- Date of birth
- Driver's license
- Pay grade / employee profile
- Mailing address
- Customer account numbers
- Customer Credit card / debit card information

In order to support the compliance team's requirements, the Bank needed to run an assessment with the goal to design polices and implement processes so that their internal environment was sufficiently protected from PII and PCI breaches.

Sensitive Data Manager Answers the Call for PCI Compliance

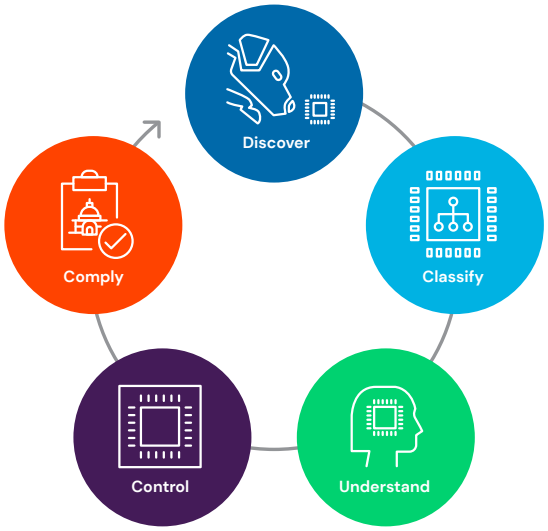
This community bank began with a data discovery/inventory of sensitive data. They required a solution that deployed centrally but discovered data anywhere on the network including remote computers, file shares, scanned images, email archives and the intranet. The Bank found Spirion to be the most efficient and detailed data discovery tool for their needs. Spirion's data discovery platform was able to accurately spot social security numbers, credit card numbers and other PII; specify the documents, the full path location, who worked on it, and even displayed a preview of where the PII was inside the document.

The compliance team reviewed the data discovery results and engaged branch management to come up with process and guidelines to review locations with PII, and more importantly, to secure those locations by informing branch associates to fix situations where Spirion discovered insecure PII. The branches were each responsible for fixing their gaps using Spirion as the tool which consistently detected and reported PII discovery. They chose Spirion because the software met some key compliance needs, such as:

- Defined and supported the process to manage data protection for the bank
- Installed and managed from headquarters while detecting and fixing sensitive data at the branches
- Prompted branch staff to fix their data in files they own and used
- Complemented existing data privacy technology with routinely scheduled scans to identify and secure employee data.

Sensitive Data Management is a Process to Maintain Compliance and Guarantee Client Trust

This use case demonstrates the effectiveness and necessity of sensitive data management within the financial services segment. An advisor, a relationship manager or any support person may lose clients' personal and financial data through multiple transport channels – files, email, web traffic, instant messaging, removable media, or a multitude of other media – so the financial institution must proactively protect client and other sensitive data. Prior to defining policies, it is critical to inventory and classify data. Spirion defines Sensitive Data Management as a process to discover and protect client data. It is not a product or a one-time project. Sensitive Data Management helps your organization understand information that:



- Places you at risk of noncompliance
- Precludes you from earning more business due to trust issues
- Disrupts your business continuity with partners, suppliers and employees
- Puts your clients at risk

As a result without a Sensitive Data Management process, your entity may suffer negative effects in quality of services, and miss out on revenue opportunities. In short, Sensitive Data Management just makes sense.

Sensitive Data Management is a Process to Maintain Compliance and Reduce Risks

Process Stage	Key Tasks	How Sensitive Data Manager Empowers Process
Discover	Find sensitive data that can be classified	Sensitive Data Manager efficiently and accurately scans your data environment and finds Cardholder data so you know exactly the size and location of your Cardholder data at rest.
Classify	Apply labels so that data can be protected	Sensitive Data Manager classifies the sensitive data automatically whether it's SSN, credit card number, bank number, or keyword match so you easily delineate the data types.
Remediate	Shrink the environment in which the data lives	Sensitive Data Manager shreds or quarantines sensitive data so your target data environment is kept small.
Enforce	Enforce the policies and procedures	Sensitive Data Manager is scheduled to continuously scan the data environment and fix unsecured data to enforce policy. Sensitive Data Manager's accuracy and efficiency makes it the best tool to deploy for enforcement.
Enforce	Create actionable policies and classifications for and effective deployment	Automated reports show trends and points out potential leakage areas. Sensitive Data Manager supplies the data to design and implement a sensitive information management strategy.

Talk to a Spirion data security and compliance expert today: expert@spirion.com

Spirion has relentlessly solved real data protection problems since 2006 with accurate, contextual discovery of structured and unstructured data; purposeful classification; automated real-time risk remediation; and powerful analytics and dashboards to give organizations greater visibility into their most at-risk data and assets. Visit us at spirion.com