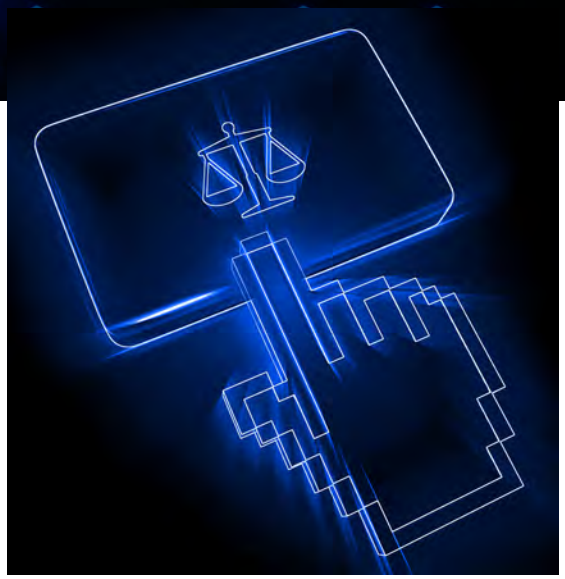
GROUND LABS

CASE STUDY

How a Leading Financial Technology Company Achieves PCI Compliance With Ground Labs' Enterprise Recon



A finance provider managing payments for thousands of businesses

A leading financial technology company that uses Enterprise Recon helps thousands of businesses increase sales and profits by offering flexible payment options for customers. The company works with a wide range of industries across North America, including veterinary, dental, continued education, and dating services industries.

> *"PCI compliance is critical for businesses handling credit card numbers because credit card fraud and theft are very prevalent."*

The search for a PCI compliance solution

This firm has more than 2 billion USD assets under management and has helped businesses finance hundreds of thousands of consumers, requiring it to handle a high volume of credit card and social security numbers every day. The company needed to ensure that sensitive data was secure, and wanted to maintain Payment Card Industry (PCI) compliance. PCI compliance is critical for businesses handling credit card numbers because credit card fraud and theft are very prevalent.

In 2019, the Federal Trade Commission (FTC) received **271,000** reports of credit card fraud in the US.[1]

[1] *"Consumer Sentinel Network: Data Book 2019," Federal Trade Network, January 2020, https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2019/consumer_sentinel_network_data_book_2019.pdf.*

Hackers are highly motivated to steal credit card data. If they gain access to sensitive data like primary account numbers, cardholder names, and authentication codes, hackers can impersonate the cardholder, use the card to make purchases, and even steal the cardholder's identity.

Companies that fail to meet their obligation for PCI compliance are vulnerable to:[2]

- Loss of reputation and consumer confidence, causing potential customers to take their business elsewhere
- Diminished sales
- Cost of reissuing new payment cards
- Fraud losses
- Higher subsequent costs of compliance
- Legal costs, settlements and judgments
- Fines and penalties from the PCI industry, card issuers, and government entities
- Termination of ability to accept payment cards
- Lost jobs (CISO, CIO, CEO and dependent professional positions)
- Going out of business

If a data breach occurred and hackers gained access to customer credit card data and social security numbers, this financial technology company could suffer from a huge financial and reputational burden. Customers lose trust in businesses after data breaches, and the costs of this add up.

To protect sensitive data and maintain customer trust, the financial technology company needed a solution to help it accurately, quickly, and easily identify where credit card and social security data was stored, allowing the company to remediate and protect the sensitive data before the data was compromised.

[2] *"Why Security Matters," PCI Security Standards Council, https://www.pcisecuritystandards.org/pci_security/why_security_matters*

GROUND LABS

An IBM report found that the average cost of lost business due to a data breach in 2019 was **$1.42 million**.[3]

[3] *"Cost of a Data Breach Report," IBM, 2019, https://www.ibm.com/downloads/cas/ZBZLY7KL*

Ground Labs' Enterprise Recon helps financial organizations maintain PCI Compliance

Because this financial technology company handles such a high volume of credit card and social security numbers, the team knew it had a monumental task ahead to find where all that data was being stored. That's why, in 2016, the team decided to partner with Ground Labs, and ever since, has relied on Ground Labs' award-winning Enterprise Recon software to meet and maintain PCI compliance.

The company uses Enterprise Recon PII to find where credit card and social security numbers are stored within both structured and unstructured data sources, including files, databases, emails, cloud, big data, and more.

An initial scan with Enterprise Recon PII resulted in 4 million matches, or 4 million places where the company was storing social security or credit card numbers, some in surprising locations. For example, the company learned that Google Chrome had been caching data without their knowledge, so it created new policies to prevent this from happening in the future.

This company uses an internal naming system that utilizes nine-digit codes, which most PCI compliance solutions would confuse with social security numbers. However, Enterprise Recon makes it easy for the team to filter those nine-digit codes out of its ongoing scans. This helps the company more accurately discover valid sensitive data and take appropriate action. This saves time and, most importantly, keeps clients' data protected.

Now, the financial technology company uses Enterprise Recon PII to run bi-weekly scans that are automatically executed according to pre-configured recurring scan schedules. After scanning for credit card and social security numbers, Enterprise Recon PII allows the team to view and analyze where sensitive data resides and immediately contact the owners to take action.

Enterprise Recon found **4 million** instances where the financial technology company was storing credit card or social security numbers.

"Ground Labs' Enterprise Recon tool is easy to use and configure, and it allows us to immediately find and remediate sensitive information at the source. With Enterprise Recon, our entire organization has become more aware of sensitive data and how to properly manage it."

— IT Network and Security Manager at a leading financial technology company

Ultimately, Enterprise Recon PII provides a blueprint of the social security and credit card number storage locations across the organization, allowing the financial company to ensure on an ongoing basis that it is not storing any social security or credit card numbers unnecessarily, and when necessary, that the company is storing them securely to protect sensitive consumer information.

The results — Ground Labs' Enterprise Recon PII helps companies:

- Identify more than 300 data types including predefined and variants that include sensitive, personal and confidential data, including credit cards, driver's licenses, passports, names, addresses, phone numbers, dates of birth, national IDs, health data and more.
- Identify data from over 50 countries.
- Broaden data searches across multiple types of data, regardless of where stored, with GLASS™ powered custom data types to discover sensitive data according to companies' unique requirements.
- Go beyond identifying — remediate with comprehensive options — encrypt, mask, secure delete, quarantine — to quickly secure and eliminate all exposed sensitive data and achieve a true zero trust security posture.

300+ data types
including predefined and variants that include sensitive, personal and confidential data

GROUND LABS

To learn more about how Enterprise Recon can enable your business to become PCI compliant, click **here.**