

BCR Collects on Compliance



“Compliance adds value at every layer of our company – and, most significantly, if it’s important to our clients, it’s important to us.”

- David Winters, Senior Vice President

Industry

Financial Services – Collections

Challenge

Bureau of Collection Recovery sought to achieve PCI compliance and also meet security requirements of their high-profile clientele.

Solution

BCR engaged services from SDS in rational, bite-sized pieces laying the foundation, brick by brick, for a solid PCI compliance stance.

Outcome

Bureau of Collection Recovery demonstrated their commitment to PCI compliance and thereby increased their appeal to their client marketplace.

Company Profile

The Bureau of Collection Recovery (BCR) was incorporated in 1986 by the Department of Banking and related Regulatory Agencies in all 50 states.

BCR is an independently owned, national collection agency. Their independence from large collection groups enables BCR to be free from the bureaucratic processes that many non-independent agencies must face on a daily basis. BCR is focused on delivering a superior level of customer satisfaction and loyalty.

Business Situation

Many of BCR’s clients are publicly traded companies who are also classified as Level 1 Merchants according to the PCI DSS 1.1 standard. This created a situation where, beyond BCR’s desire to be compliant for their own internal processes, they saw an opportunity to differentiate themselves in the marketplace and serve their clients at a higher level.

Like many managers, BCR’s management team was aware of several elements of the PCI puzzle and also understood that they needed to learn what they did not yet know before deciding on the most appropriate path for achieving compliance.

Hiring a company to come in and run the “PCI playbook” was not a viable option for BCR - they wanted to develop a comfortable approach to compliance and build confidence with their PCI compliance partner along the way.

Solution

BCR chose to engage SDS to apply its services in a step by step approach. Because SDS was able to offer its services in an ala carte fashion and not a one size fits all playbook approach, BCR was able to gain confidence in SDS’s abilities with very little risk.

SDS first delivered a detailed analysis of BCR’s information security policies. Activities in this phase included:

- Detailed reviews of current policy documentation
- Policy content recommendations based upon the detailed reviews
- Recommendations regarding gaps in current policy and scope of the Information Security Program manual.

Deliverables to BCR from this phase included:

- A comprehensive baseline document and realistically actionable recommendations based upon analysis of current policy documentation to align with PCI requirements and industry best practices.

continued . . .



... “BCR Collects on Compliance” continued

Pleased with the first deliverable, BCR then invited SDS to undertake a second project developing a log management standard to align with PCI requirement number 10. Activities in this phase included:

- Development of a log management standard using the previously delivered Bureau of Collection Recovery policy template.
- Reviews of up to ten in-scope systems for logging configuration capabilities and document current gaps in logging practices
- Reviews of log management standards with Bureau of Collection Recovery personnel for completeness, accuracy, and knowledge transfer.

Deliverables BCR received from this phase included:

- Log management standard addressing log configuration requirements of operating systems and network devices that meet PCI DSS 1.1 requirements.
- Notes from system log configuration review indicating where log management gaps exist for PCI audit requirements.

And, once again being pleased with the prior work, BCR requested that SDS review the process by which cardholder data is stored and provide recommendations as to how this data is used and stored to meet PCI requirements. Activities in this phase included:

- Review of current credit card data flow through BCR’s primary core application
- Collecting, organizing, and defining an understanding of controls in place around the use and storage of cardholder data in the core application.
- Providing recommendations to improve controls of stored and transmitted cardholder data within the core application.

Deliverables from this phase included:

- Documentation outlining the use and storage of sensitive cardholder information within BCR’s core application and pragmatic recommendations for controls to meet PCI compliance requirements and align with industry best practices.

Outcome

BCR has enhanced their marketability and appeal through achieving a *comfortably compliant* stance for PCI Merchant Level 1.

BCR has developed new support for successful growth by constructing a *scalable and maintainable compliance framework* that supports their business growth objectives.

BCR has insured the future value of their company by moving beyond point compliance and undertaking a *continuous compliance* mindset.

For Comfortable Compliance

Please contact: sales@securedigitalsolutions.com