CASE STUDY

Helzberg Diamonds Reduces PCI DSS Scope in its Back Office by 98 Percent

Helzberg Diamonds® is one of the oldest, most respected jewelry retailers in the United States. Founded in 1915 and headquartered in North Kansas City, Missouri, the Berkshire Hathaway company has grown to 2,500 employees. Today, it sells exclusively designed fine jewelry through its ecommerce site and 234 retail stores nationwide.

In 2009, Helzberg began exploring data security strategies to comply with the Payment Card Industry's Data Security Standard (PCI DSS). Helzberg needed a solution that would provide strong protection throughout its extended enterprise with a minimum of disruption to its processes. The retailer's POS systems were encrypting credit card data at the stores, but once the numbers were decrypted at headquarters there was no way to re-encrypt them for storage in back-end systems without having to manage multiple keys. Helzberg first turned to its POS and sales audit system vendor for suggestions. After considering several encryption options, the IT department chose Liaison technologies.

"We chose Liaison because they had worked with our POS vendor in the past and had an encryption solution that would allow us to generate keys and send them down to the POS systems," said Florian Yanez, Helzberg Diamonds' Manager of Technical Systems. "This would allow us to decrypt and re-encrypt the data as we needed to on the back- end, without having to generate new keys."

Implementation Planning Yields a Change in Strategy from Encryption to Tokenization

The process started with Liaison's three-day Architecture Design Workshop, which explored Helzberg Diamonds' situation and resulted in a customized data protection strategy and a blueprint for deployment.

"Going into the workshop, our thought was just to keep the data encrypted," said Yanez. "We were preparing to implement a new version of our sales audit system that would allow us to store encrypted data generated by the POS systems. It had a built-in decryption routine that would allow employees to decrypt credit card numbers on the fly within the sales audit system. However, that didn't solve the problem for our other back-end systems." When the POS and sales audit software vendor declined to give Helzberg access to its proprietary encryption/decryption code so they could use it with other systems, they were forced to look at other options.

"We learned of this roadblock during our implementation planning phase with Liaison, which caused us to realize that our best course of action would be to take control of the data as it comes up from the stores by encrypting it ourselves so everything is encrypted in the same way throughout our organization," said Yanez. "It was then that we realized

Quick Facts

Company

Helzberg Diamonds

Kansas City, Missouri

www.helzberg.com

Industry

Retail

Liaison Solution

Liaison Protect

"Liaison's tokenization removed 98 percent of our 400 back-end systems from scope for PCI DSS compliance and gives me great confidence that our customers are well protected."

— FLORIAN YANEZ
MANAGER OF
TECHNICAL SYSTEMS

that Liaison Protect Token Manager, which we had originally licensed to tokenize social security numbers stored in our database, could solve our problem."

Instead of using an encryption key generated by the POS system, Helzberg now distributes a Liaison encryption key out to the POS system so that when a credit card is swiped at a store it is encrypted by the POS system using a Liaison key. This simplifies key management by allowing Helzberg to use a single set of keys to protect sensitive credit card numbers from the time they enter the POS system all the way to their back-end systems – no matter what application or database holds the data.

"We then realized that if we tokenized the credit card numbers and moved all of the processes that handle encrypted or decrypted card data into a separate PCI zone, most of our back-end systems would fall out of scope for PCI DSS compliance," said Yanez. "To make sure we were on the right track, we asked a QSA to review our plan, even though at our level we can do self-assessments."

Another advantage of Liaison's Format Preserving Tokenization, which generates tokens that fit into existing data field sizes, was that Helzberg was able to implement it without modifying its back-end systems. Only interfaces to outside companies needing real credit card numbers were modified. Yanez explained, "If we had decided to store encrypted data instead of Format Preserving Tokens, we would have had to expand the data fields to accommodate the larger encrypted values, and we would have also required a system to decrypt the data when needed. Using tokens in place of the credit card numbers gives us more control over the processes that use the numbers, as well as who accesses the data and how."

Encrypted credit card numbers are now sent nightly via a virtual private network (VPN) to Helzberg's headquarters, using the polling server which then sends them into a file processing routine that looks at the files to determine where they need to go and whether they need to be decrypted and tokenized. If the data needs to be decrypted, it's done automatically and then tokenized.

The tokens are then sent to the back-end applications and databases and the original credit card number is encrypted and stored in a central data vault. Although a rare occurrence, when an authorized employee does need to see a credit card number, they can enter the token to retrieve the credit card number.

The Result: A 98 Percent Reduction in Back-Office System Scope

"Liaison's tokenization removed 98 percent of our 400 back-end systems from scope for PCI DSS compliance and gives me great confidence that our customers are well protected," said Yanez. "Tokenization made it much easier for us to segment off our systems so that now only ten remain in scope, including the tokenization system and the one application that allows employees to redeem the actual credit card for the tokens."

Atlanta – US HQ
3157 Royal Drive
Building 200, Suite 200
Alpharetta, GA 30022
Tel +1.866.336.7378
+1.770.442.4900
Fax +1.770.642.5050

United Kingdom
+44 (0) 1425 200620

Finland
+358 (0)10 3060 900

The Netherlands
+31 (0) 20 700 9350

Sweden
+46 708102213