CASE STUDY

Validated Point-to-Point Encryption (P2PE)™ Solution

THE MERCHANT

THE HILLMAN GROUP

Established in 1964, The Hillman Group provides an array of products for commercial and residential uses to over 21,000 businesses including Lowe's, Home Depot, PetSmart, PETCO, Sears, Ace Hardware, True Value, and Walmart. Hillman is the leader in today's market in fasteners, keys, letters, numbers, signs (LNS), and engraving.

THE P2PE SOLUTION

Bluefin Payment Systems

Founded in 2007 and named the 6th fastest growing U.S. company by *Inc. 500* in 2012, Bluefin Payment Systems provides secure payment technologies to 16,000 enterprises, financial institutions and small-medium sized businesses worldwide. Bluefin built the first P2PE Solution to be validated by PCI SSC in North America as well as the first mobile P2PE Solution.

THE OBJECTIVE

The Hillman Group selected Bluefin to implement its PCI-validated P2PE Solution in its 4,000 automated custom engraving kiosks in order to reduce the number of applicable PCI DSS requirements for their CDE, secure their retail transactions and protect their brand from a costly card data breach.

Protect the Customer. Protect your brand.

Let's hear from the Merchant and the P2PE Solution Provider.

What does P2PE accomplish for The Hillman Group?

Hillman Group: We operate thousands of self-service kiosks in North America that accept card payments every day. We used Bluefin's P2PE Solution to reduce the number of applicable PCI DSS requirements for our cardholder data environment (CDE) and to provide the most secure technology possible for our customer's data.

Bluefin: Maintaining over 230 security requirements from the new PCI SAQ D for each kiosk not only presented a logistical challenge, but was also costly in terms of maintenance. Hillman used P2PE to reduce the number of applicable PCI DSS requirements and qualify for the new PCI DSS SAQ P2PE with 26 security requirements. Malware in the POS (point-of-sale) system is responsible for many retailer card data breaches over the last two years. A PCI-validated P2PE Solution includes SRED (Secure Reading and Exchange of Data) technology which encrypts card data at the point of entry with a unique key per transaction, protecting the data before it reaches the POS where it could be exposed to malware.

**Note: Check out PCI SSC's infographic titled Protecting Your Customer's Payment Card Data from Malware for more information.*

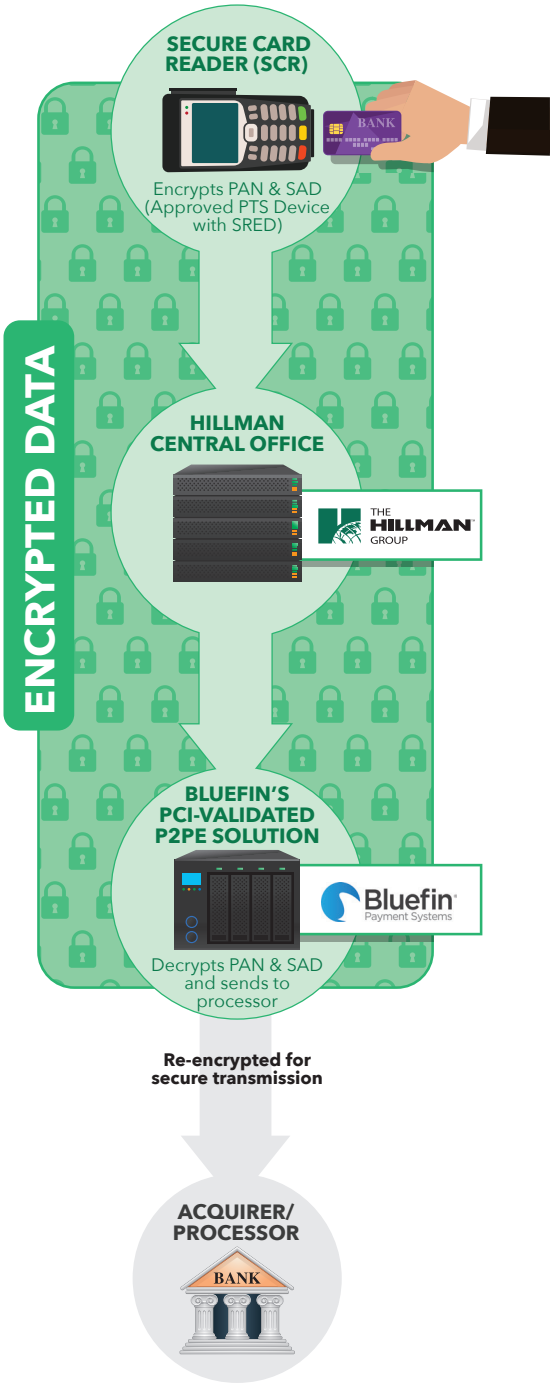
Why did you choose Bluefin's P2PE Solution?

Hillman Group: Some providers are selling their P2PE solution as "fully secure" despite lacking accreditation by the PCI Security Standards Council. Our research led us to PCI's FAQ which states, "Only Council-listed solutions are recognized as meeting the requirements necessary for merchants to reduce the scope of their cardholder data environment (CDE) through use of a P2PE solution." Bluefin is a Council-listed P2PE Solution provider in North America.

Bluefin: Some non-validated vendors offer devices with SRED hardware encryption. A validated P2PE Solution goes beyond SRED-enabled devices to require hardware key management at the solution provider, chain of custody management for devices, P2PE-validated key injection facilities and more. We researched whether such SRED devices alone could provide CDE scope reduction and found this in the PTS Security Requirements Version 3.0 FAQ: "SRED is not in itself an answer to how to deploy point-to-point encryption, but is an important first step covering encryption at the point of entry."

CASE STUDY

Validated Point-to-Point Encryption (P2PE)™ Solution



PAN = Primary Account Number SAD = Sensitive Authentication Data

Was there concern for security given the onslaught of data breaches?

Hillman Group: Clearly the amount and severity of security breaches is a cause for concern. Companies such as ours need to understand the latest security products to take care of our customers and to protect our brand. We wanted to ensure that we are taking care of our customer by holding their personal data in the most secure manner. Such security is also valued by our retail partners.

What roadblocks did you have to overcome?

Hillman Group: The largest roadblocks were technology based. We needed to develop and validate a P2PE solution that functioned properly with the variety of products that we offer. We also worked to find a provider that could grow and change with us in the future. Bluefin met those requirements.

Bluefin: Implementing and managing several thousand P2PE devices could present a logistical challenge. Hillman used P2PE Manager, Bluefin's chain of custody management system, to ease the implementation and ongoing management process and to comply with SAQ P2PE's PCI DSS requirements.

What would you say to other companies that might be thinking of implementing a P2PE Solution?

Hillman Group: It's important that companies understand the security threats and the solutions available. We hired a professional consultant to help us develop the best solution for our situation. This is an area in which you cannot grow complacent – the technology is ever changing.

> *We're excited to offer a world class payment processing system that ultimately provides our customers with sound peace of mind. It's been a pleasure working with Bluefin to develop a strategy, technical solution and action plan to achieve our final product.*
>
> **Todd Spangler**, SRVP & General Manager, The Hillman Group

> *Card data breach security is not a one-product-fits-all selection. Card data exists in various forms in merchant systems and is exposed to vulnerabilities that a single security product simply can't address. Rather than build higher walls and stronger security measures, Bluefin recommends that merchants devalue the card data in their systems rendering it useless to hackers. A holistic approach to devaluing card data which includes a P2PE solution, can not only protect the data roundtrip, but may also reduce the total cost of compliance by potentially reducing PCI DSS CDE scope.*
>
> **Ruston Miles,** Founder & Chief Innovation Officer, Bluefin Payment Systems

Maximize Security. Simplify Compliance.

Validated P2PE Solution Providers can be found on the PCI website at:
http://www.pcisecuritystandards.org/p2pe