Luxury Daily®

The News and Intelligence You Need on Luxury

RESEARCH

Sophisticated hackers call for refined payment security systems: report

February 19, 2016

Value Retail promotional image

By SARAH JONES

As retailers innovate and enhance the omnichannel shopping experience, one of their biggest challenges will be creating an inclusive payment security strategy, according to a new report by Boston Retail Partners.

Subscribe to Luxury Daily
Plus: Just released State of Luxury 2019 Save $246 ›

Payment security is one of the top concerns for retailers today, with hackers becoming more sophisticated and even high-profile institutions falling victim to data breaches. In order to protect themselves, brands need to update and strengthen their security systems, which may now be out-of-date.

"Hackers and fraudsters are in a constant back and forth with retailers as it relates to payment security," said Ryan Grogman, vice president at Boston Retail Partners. "As retailers close certain loops, the hackers move on to the next most vulnerable spot in the transaction, and retailers are then forced to develop new measures to address the weakness.

"This cycle has been going on for many years, and the biggest change in payment security today is the sophistication and level of technology available to both sides," he said. "The advent of PCI standards really moved the needle forward in terms of retailer defenses, but even with these controls in place, we are seeing high-profile retailers subjected to massive data breaches and the associated public relations fallout.

"For the card issuers and banks, they are driven by a need to reduce the amount of fraudulent charges. For retailers, it is the fear of being the next company in the headlines for a breach along with having their valued customers' sensitive information exposed that is driving many of these changes. EMV is another attempt by the issuers to deflect the fraud liability back to retailers, and that financial liability has driven many retailers to allocate more budget to enhance payment security and implement EMV."

Boston Retail Partners' "Payment/Data Security in an Omnichannel World" is based on data from the consultancy's 2016 POS/Customer Engagement Survey.

Payment plan

Boston Retail Partners' survey found that most retailers are planning to implement a multi-tiered security strategy. Most effective is combining end-to-end encryption with EMV transactions.

EMV-enabled credit cards include an embedded chip, which a compatible terminal can read to verify that it is the original issued card. This prevents the use of fraudulent or counterfeit cards.

Today, only 22 percent of retailers support EMV transactions, up from 10 percent last year, but another 53 percent plan to have EMV in place within the next 12 months. The burden of liability surrounding EMV shifted in October, and now payment networks hold merchants in the United States accountable for fraudulent transactions surrounding chip cards if the retailer does not support EMV.

Bloomingdale's Palo Alto store

EMV may lower the probability of a thief using a fraudulent physical card in a transaction, but EMV compatibility alone does not do anything to mitigate the risk to the data once a card has been swiped. End-to-end encryption (E2EE) works from the swipe.

Almost half of retailers have implemented E2EE. Boston Retail Partners suggests keeping the encryption key with the bank or switch provider, putting it outside of a retailer's system entirely, thereby eliminating the possibility that a hacker could decrypt data within the store's environment.

Similarly, tokenization turns all data, including credit card numbers, into tokens. At the transaction, the card number is translated into a token, which cannot be converted back. Again, retailers should let the token vault, which generates the token string, be housed outside of their system.

Once a consumer has completed a purchase with a particular card, her token should be used again for every purchase across channels, allowing the store to seamlessly identify her without needing to include credit card information. Twenty percent of retailers have adopted tokenization, with an additional 22 percent planning to add the feature within a year.

"Luxury retailers win a majority of their most valued customers through establishing a relationship built on personalization and trust," Mr. Grogman said. "With that loyalty can come a lifelong relationship, but it is essential that the customer trusts the retailer to value their needs, preferences and most importantly their personal information.

"With higher per-item retail prices and higher transaction totals, the customer base itself will skew towards higher limit credit cards," he said. "It becomes essential to protect this sensitive payment data by employing the latest technology trends in end-to-end encryption and tokenization so that nowhere in the process can hackers gain access to this sensitive information."

Samsung Pay powered by Mastercard

Mobile payment offerings using near field communications are on the rise, with Apple Pay adoption doubling in the last year to 16 percent of retailers. As consumers opt to use their phones more throughout the in-store shopping experience, retailers need to ensure that the information they are sharing, such as recently browsed items, store account profile and purchase history, is secure.

Retailers will be more successful in the mobile payment space if they earn consumers' trust and provide incentives for them to use their mobile devices at checkout.

When it comes to physically moving data, about half of retailers use a semi-integrated or non-integrated terminal, both of which do not communicate credit card data to the POS application, instead sending it directly to the bank or issuer for authorization. This tendency is growing, and more retailers are expected to switch to a semi-integrated terminal over the next yea, due to the limitations the non-integrated terminal presents.

Those who do use an integrated terminal tend to use switches or gateways to route the payment information to the right bank or processor. Most of these paths are in-house, but they can also be owned and operated by a third party vendor, an option more retailers will likely take as they try to remove data from their own system.

Ecommerce environment
Security is not only an issue in-store, especially as online shopping becomes more popular. Additionally, if retailers implement tougher security systems at the physical point-of-sale, criminals are apt to move their focus online.

According to Trustev, online fraud is expected to rise 106 percent over the next three years.

Fashion ecommerce has shown no signs of slowing, with online purchases expected to more than double to $3.5 trillion by 2019, and with that, fraudulent sales have kept up the pace, according to a new report by Riskified.

Riskified's "Fraud in Online Fashion" report is geared toward ecommerce retailers selling premium and luxury fashion brands in the online space. For an industry that counted $8.5 billion in online sales for 2015, a figure expected to double by 2020, online retailers must be aware of the increasingly difficult challenges and risks the counterfeiting underworld presents (see story).

Unlike in-store, one it becomes hard for brands to tell whether the card being used is actually the purchaser's without the help of a chip, signature or identification.

Therefore, retailers have to rely on an automatic monitoring system that audits purchases that are suspect and enables legitimate transactions to go through. Manual auditing is clunky in today's ecommerce environment where consumers expect services such as same-day delivery.

Instead, brands should be learning about their consumer profile to be able to flag suspicious transactions, leveraging available data from past transactions and looking at trends.

In an effort to make online shopping simpler, retailers often store consumer credit card information, sparing the shopper from entering her card number each time she returns. While this could open a consumer's data up to hackers, a number of retailers that use tokens in-store are also leveraging them online, protecting consumers across channels.

"The most effective approach for securing payment card transactions is the multi-tiered approach of implementing end-to-end encryption, tokenization, support for EMV, in addition to a rigorous set of security protocols," Mr. Grogman said. "For ecommerce transactions, those additional controls may come in the form of advanced fraud management through the use of tools, retailer-specific business rules and rigorous monitoring.

"As it relates to omnichannel, there is an expectation on behalf of the consumer that they can buy anywhere, return anywhere and ship anywhere at anytime and the overall experience should be relatively seamless across the various channels," he said. "Sometimes advanced security controls make it challenging to support such an experience, so retailers should evaluate the impacts on their cross-channel practices when designing payment security programs.

"One key example is the use of tokenization. By replacing card values with meaningless token values, retailers can greatly reduce their risk of a breach; however, if these tokens are not similar across channels or if they are uniquely generated for every swipe of the same card, then retailers will be hamstrung when it comes to efficiently processing cross-channel returns or transaction lookups by credit card. An omnichannel, multi-use token addresses this scenario and has become the best practice for forward thinking retailers."

© 2020 Napean LLC. All rights reserved.

Luxury Daily is published each business day. Thank you for reading us. Your feedback is welcome.