CNP CardNotPresent.com
THE INDEPENDENT SOURCE FOR ORIGINAL CNP NEWS

Experian

EMVersary: EMV's Impact on Card-Not-Present Commerce One Year Later

THE CNP REPORT

October 18, 2016

CardNotPresent.com

By Karisse Hendrick, Editor-at-Large, CardNotPresent.com

On October 1, 2015, Visa and Mastercard changed the liability rules in the United States for fraudulent credit card purchases at card-present locations as an incentive for issuers and merchants to issue and accept EMV/chip-enabled cards. Fraudsters had learned how to easily transfer stolen card data onto cards with magnetic strips, making counterfeit fraud an estimated $4.5 billion dollar problem. While issuers previously had covered the cost of these losses, the liability shift of a year ago placed that burden on merchants with credit card terminals not yet enabled to accept chip cards. If merchants are compliant, but the issuer has not issued chip cards, the issuer foots the bill.

While the actual implementation of EMV was a card-present concern, experience from other global markets that had made the switch suggested the move would have a significant impact on card-not-present fraud rates. In the U.K., CNP fraud rose 79 percent in the first three years of EMV and it more than doubled in Australia. It became apparent in those countries that most fraudsters who made a career out of utilizing stolen credit cards didn't suddenly decide to get a day job.

Thus, CNP merchants in the U.S. were warned to expect the same. A year after the U.S. liability shift, it's apparent that the EMV shift in the card-present markets has significantly impacted CNP fraud rates and fraud departments while lowering card acceptance rates for subscription-based merchants and increasing security threats to CNP companies. And more importantly, because this conversion is not complete, we learned how merchants can better prepare themselves for the continued problems headed their way.

EMVersary: EMV's Impact on Card-Not-Present Commerce One Year Later

The State of the Card-Present EMV Conversion

A recent study by the Strawhecker group found that 29 percent of card-present merchants are equipped with an EMV-compliant terminal and the appropriate software to process chip-card transactions. More issuers raced to become EMV compliant than merchants this past year: 64 percent of Visa cards and 88 percent of Mastercards now include a chip. Because so many merchants still do not have the correct terminals and software to accept chip cards, Mastercard has seen counterfeit fraud increase 77 percent for those businesses, as credit card fraudsters move to a "weaker link" and likely push stockpiles of counterfeit cards through these systems before all card-present credit card terminals are converted.

The Impact on CNP Fraud... So Far

Even though non-EMV-compliant merchants are experiencing a "trickle-down" effect of counterfeit fraud, many fraudsters have already migrated to the next path of least resistance, card-not-present channels. While the EMV conversion impacts cards issued in the U.S., fraud attributed to this change is not isolated to U.S. CNP merchants. When the U.K. converted to chip cards, the impact of fraud was felt globally, with approximately one-third of all fraud on U.K.-issued cards occurring in the U.S., and another third occurring abroad.

The rate of fraud experienced this year by card-not-present merchants varies based on the companies reporting the upticks. While Forter recently released a study showing fraud attempts on their network increased by 137 percent in the last year, Experian's Global Fraud & Identity group has observed close to 20 percent increase in 2016 over 2015. This difference could be based on a range of factors, but one thing on which all companies that have measured these rates agree is that CNP fraud attempts have risen significantly since October 2015.

And, as fraud attempts go up, according to David Britton, vice president of Industry Solutions at Experian, the percentage of sales being compromised is also rising. That increase can have a negative impact on your internal fraud processes and your good customers, Britton warns. Experian saw an average fraud attempt rate of 1.2 percent of sales in 2009. However, post EMV, fraud attempts are now closer to 3.2 percent of a CNP merchant's sales. Britton also notes that while they attribute a large percentage of this increase in fraud to the EMV liability shift, there also is a "rate of expected increase through organic growth and migration of consumers to CNP channels. Fraud is not linear. You may see sales increase by 5 percent, but fraud grows 7-10 percent," he says. "The bigger the haystack, the harder it is to see the needles."

When CNP merchants see an increase in sales in tandem with and increase in fraud attempts, Britton says many tend to "either tighten rules (in a rules-based engine) or throw bodies at the problem [to perform more manual reviews]. Merchants relying on manual reviews to identify or verify fraud are looking at an industry average of 27 percent of their orders, in order to catch the 3.2 percent of the transactions that are actually fraudulent. You have to have a bucket bigger than the problem, in order to catch it [when relying heavily on manual reviews]." Britton points out that if you're reviewing 27 percent of your company's orders and only 3.2 percent are fraudulent, you may be negatively impacting 24 percent of your good customers by delaying and/or canceling legitimate orders, causing lost sales and a poor customer experience.

Fraud Methods are Changing

Beyond an increase in fraud attempts, many fraudsters are changing tactics based on the information available on the dark web. While breaches in 2014 were primarily focused on comprising credit cards in physical locations (think Target and Home Depot breaches), many breaches in 2015 targeted industries rich with personal consumer and/or account information available online (e.g., government agencies like the Office of Personnel Management and health insurers such as Premera and Anthem).

"The biggest impact we have seen is that e-commerce has become more of a target for hackers. EMV acceptance makes the card data much less valuable to hackers and fraudsters," says Mike Petitti, senior vice president of Global Alliances at cybersecurity firm Trustwave. "Therefore, e-commerce merchants tend to be targeted more as the EMV rollout continues."

This is important information for security teams, charged with securing the personally identifiable information (PII) of their customers. This also can explain why the methods by which fraudsters are attempting to defraud CNP merchants are changing at a rapid pace.

When credit cards were most available on the black market, merchants often saw what is sometimes referred to as "clean fraud"—fraudsters opening new accounts or checking out as guests utilizing stolen credit cards. As companies worked to deter that kind of fraud and secure payment card information, the data available on the black market changed from credit card numbers to PII such as social security numbers, past addresses, phone numbers, employer, etc. and account information such as e-mails, user names and passwords. At the same time, the types of fraud CNP merchants see are changing as well. In a 2015 report, Javelin Strategy & Research published a study that predicted account takeover fraud and account creation fraud would increase more than 60 percent by 2018. While these two fraud methods accounted for an estimated $5 Billion in losses in 2014, they are expected to reach $8 Billion in 2018.

Recommendations to Reduce Fraud Losses during "Perfect Storm" of CNP Fraud

When fraud losses and manual review rates increase in tandem with fraud attempts and changes in fraud tactics, it may be time to review the systems and internal processes your company is relying on to weather the storm of EMV and increased sales in CNP channels.

Britton suggests asking yourself, "What is the first filter or system designed to do the heavy lifting in identifying fraud, and is it working?" He warns that if EMV has already caused a strain in resources and impacted staffing and good customers (through false positives), the holidays could be very rough, indeed. But a strong "first filter," along with an overall process that catches fraud before fraudsters reap the rewards, will be a deterrant against future fraud. After a merchant has had a strong process in place "we see lower fraud attempts because the fraudsters get tired and give up," Britton concludes.

If replacing or implementing a new "first filter" is not an option for your company, you can consider layering an additional tool that identifies fraud through device identification, machine learning capabilities or through implementing 3DSecure/Consumer Authentication. Many merchants credit these types of tools to reducing the volume of orders that require manual reviews, while still utilizing currently implemented systems. There are also identity verification tools that can speed up the manual review process by verifying a customer's shipping address, e-mail or phone number. These primarily work for physical goods retailers and aren't always accurate in identifying account takeover fraud.

Another Side Effect: More Declines for Subscription Merchants

In the fall of 2015, Netflix publicly blamed the mass EMV conversion for a steep reduction in Q3 sales. In their earnings report for that quarter, this top subscription-based merchant attributed a reduction in profits "to slightly higher-than-expected involuntary churn (inability to collect), which we believe was driven in part by the ongoing transition to chip-based credit and debit cards." Melanie Stout, vice president of Client Success at Paul Larsen Consulting, says this issue is not isolated to Netflix.

"From 2013 to end of Q3 2016, all of our clients combined have experienced a 30 percent decrease in approval rates, despite best practices being in place," Stout says. "The trend has been more drastic since the onset of the EMV re-issuance. Invalid account number declines are coming in at higher volumes than they did in the wake of the disastrous Home Depot and Target data breaches."

Most merchants with recurring transactions rely on account updater tools offered by merchant processors on behalf of the card brands. But, not all issuers participate in the program and while it is financially beneficial to continue to charge the new cards that could have led to canceled accounts, there is a cost associated with receiving updated card numbers.

"When looking at the successful account updates delivered to our merchants in 2015, the volume is nearly double what they received in 2014," Stout continues. "These updates include new expiration dates as well as new account numbers, and this increase is largely attributed to chip cards."

What Will the Next Year Bring?

Only 76 percent of U.S.-issued Visa and Mastercard credit cards currently carry EMV chips. And, for debit cards, it's only 50 percent. With close to 60 percent of all card-present locations unable to accept EMV transactions anyway, the conversion process is far from over. Many experts have warned that as more merchants are able to process chip-enabled cards and as issuers move to convert 100 percent

EMVersary: EMV's Impact on Card-Not-Present Commerce One Year Later

of all Visa and Mastercard cards, almost all fraud that has been hitting physical locations will move online. The mass reissuance of cards also will continue to affect the decline rate for merchants that keep cards on file or that leverage a subscription model.

If these issues are impacting your business now, they will continue to. If your business has not yet seen an uptick in fraudulent attempts or declined transactions, chances are you will soon. It's important to evaluate your current processes and the systems your business relies on to prevent fraud, optimize declined transactions, and protect your customer's data. Other countries' experience suggests there is very little light at the end of the tunnel. Stout reminds us that even after the U.K. had fully transitioned to EMV, "they saw an 18 percent increase in card-not-present payment fraud in 2015 over 2014." Even after all cards and terminals are EMV compliant, this will be our new normal.

About Experian

EFFECTIVE FRAUD PREVENTION DOES MORE THAN PREVENT FRAUD

Fraud prevention is about more than stopping fraud. An effective program also makes it easier for your good customers to do business with you. So how do you achieve both? It starts with moving away from a one-size-fits all approach. Instead, you should apply the right level of protection needed for each transaction.

Our fraud team – nearly 300 experts around the world – focus on helping businesses do exactly that. We're proud of the fact that we helped businesses screen more than 15 billion fraud events this past year. That's over 3,300 events per second. Most consumers aren't aware of what's happening behind the scenes to keep them safe while they shop online or check bank balances from a mobile device. We call that hassle-free, and that's how it should be. Our solutions are built using data, technology and analytics to stop fraudsters without stopping good customers. Now, fraud prevention contributes to growth and a positive experience.

To find out more about our company, please visit www.experianplc.com or watch our documentary, "*Inside Experian*."

About CardNotPresent.com

CardNotPresent.com, part of the RELX Group, is an independent voice generating original news, information, education and inspiration for and about the companies and people operating in the card-not-present space—one of the only sources of content focused solely on this growing segment of the payments industry. Our only product is information. Our only goal is to provide it in an unbiased manner to our subscribers. The company's media platforms include the **CardNotPresent.com portal**, the hub for news, information and analysis about the payments issues that most affect merchants operating in the space; the **CNP Report**, an e-newsletter delivering that focused information directly to your email inbox twice a week with no extraneous clutter; the **CNP Expo**, an annual gathering of the leading companies in the space from the smallest e-commerce Websites and technology providers to global retailers and payment processors; and the **CNP Awards**, an annual event honoring the products and solutions CNP merchants rely on most to increase sales. For more information, visit www.CardNotPresent.com.