Industry Facts

Card-Not-Present Transactions

This white paper will address the truths about Card Not Present Transactions, How your business will be impacted and what you can do to eliminate your risk and fraud liability.

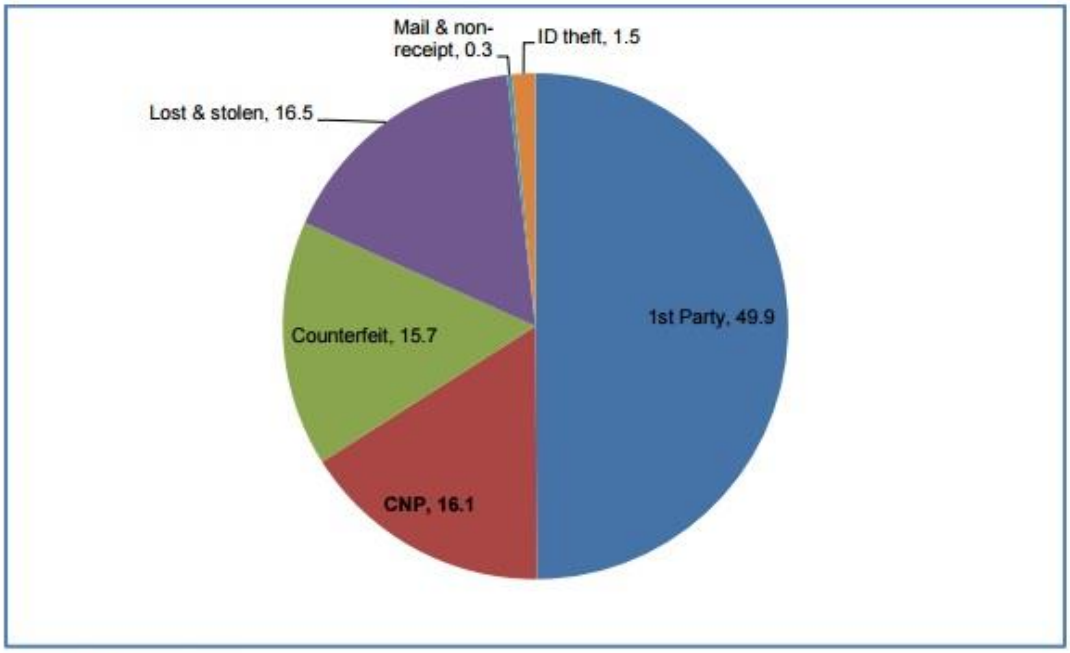
Card-Not-Present (CNP) – What does CNP and the US adoption of EMV have to do with each other. Everything! The primary purpose for the adoption of EMV in the US is to drastically reduce fraudulent activity associated to Card Present Transactions. This includes typical things such as stolen and counterfeit cards.

EMV will make it much more difficult for thieves to be successful with Card Present Fraud. In fact, after 10 years into Europe's adoption they saw fraud reduce by more than 75%. Unfortunately as Europe pushes to complete this adoption the US has been witness to a 47% increase in fraud.

While the reduction in Card Present Fraud has substantially decreased through more and more adoption it has had the exact opposite effect on Card-Not-Present transactions. Within the first few years of EMV adoption, Australia saw their CNP fraud jump from $140M in 2009 to more than $330M in 2012. The UK saw a similar spike from 2004 to 2008 where fraud escalated from $151M to $329M. These types of statistics are very similar across countries that continue to roll out EMV.

Basic tools have been presented to the market place to help protect merchants from online fraud such as Address Verification (AVS) and Card Validation Values or CVV. The US processes more than half of the world's credit card revenue so it will be no surprise that the thieves and hackers will target CNP transactions more heavily in the US. These tools have proven to be ineffective.

FIGURE 1



Source: Aite Group

Figure 1. Fraud Losses by Category

According to a 2012 report recently released by Nilson,[5] card fraud losses in the United States totaled over $5.3 billion last year. Of that amount, an estimated 36 percent, or $1.92 billion, was borne by merchants. CNP fraud represented the largest category of losses for merchants. A Cybersource report found that e-commerce fraud is equal to 0.9 percent of e-commerce revenue, a higher proportion than for other forms of commerce.[6] In addition, a recently issued data by FICO shows that CNP fraud is growing faster than counterfeit fraud.[7] Statistics from different sources may vary, but there is clearly a large—and increasingly real—potential for losses due to CNP fraud.

"The implementation of EMV in the United States presents a number of challenges. However, overcoming these challenges and completing a successful rollout will substantially reduce counterfeit card fraud at the POS. An indirect but predictable consequence, however, is that the incidence of fraudulent CNP transactions will probably increase. A number of countries that have adopted EMV have seen increases in CNP fraud. For the United States, the problem is potentially exacerbated by the increasing amount of e-commerce transactions, as opposed to traditional face-to-face commerce."

Payments Council - SmartCardAlliance

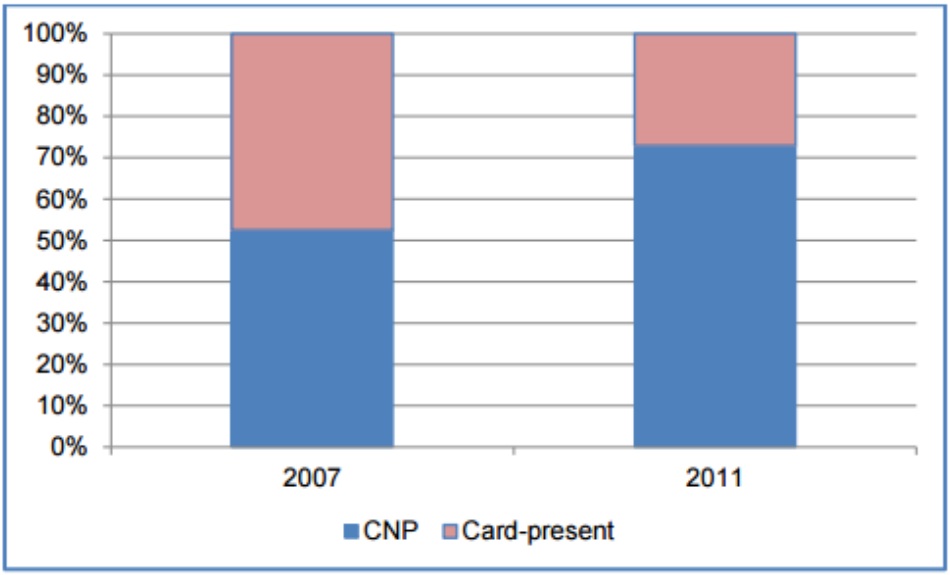
Worldwide EMV Chip Card Deployment and Adoption*

	2013		2014	
Region	EMV Cards	Adoption Rate	EMV Cards	Adoption Rate
Canada, Latin America, and the Carribbean	471M	54.2%	544M	59.5%
Asia Pacific	942M	17.4%	1,676M	25.4%
Africa & the Middle East	77M	38.9%	116M	50.5%
Europe Zone 1	794M	81.6%	833M	83.5%
Europe Zone 2	84M	24.4%	153M	40.4%
United States	-	-	101M	7.3%

*Figures reported in Q4 2013 and Q4 2014, respectively, and represent the latest statistics from American Express, Discover, JCB, MasterCard, UnionPay, and Visa, as reported by their member institutions globally.

In short, EMV adoption is coming and so is the rise in CNP transactions in the US. The way your company eliminates sensitive cardholder data while still providing the same customer experience will be a key challenge to all organizations. Providing Authentication, Encryption / Tokenization while adhering to new PCI regulations for both Card Present and Card Not Present Transactions will create enough confusion for many merchants to ultimately do nothing. Leaving them willfully non-compliant and at extreme risk.

The Observatory for Payment Card Security published similar data for France covering the years 2007–2011.[12] CNP fraud increased substantially (Figure 3).



Source: Observatory for Payment Card Security

Figure 3. CNP Fraud Amount in France after EMV Adoption

"Criminals will often go after the weakest link in the chain. Many countries that have implemented EMV chip payments have reported fraudsters shifting their attention away from the physical POS to e-commerce channels where it's much easier to make fraudulent purchases. It's important that the U.S. payments industry be proactive and evaluate ways to strengthen the security of CNP channels at the same time as the payments industry migrates to higher levels of security in-store with EMV chip technology". ***EMVCO.COM***

"Security and fraud are two sides of a very important and paradoxical coin for card-not-present merchants and the ecosystem of companies that support them. Simultaneously, they're intimately entwined and completely separate. One feeds the other: a seemingly unending parade of network security breaches is providing criminals around the world the ammunition to turn increasingly creative fraud techniques into quick profits. E-commerce and other card-not-present merchants live in constant fear of network security breaches, which they hope never come, and in the constant presence of fraud, which they battle every day to protect their bottom lines. Over the next few months, the industry will undergo major changes that affect both". ***CardNotPresent.com***

"As EMV migration proceeds, it is critical for the U.S. payments industry to take proactive steps to assist with mitigating the potential increase in CNP fraud. Identifying best practices strategies for merchants, evaluating industry-wide approaches that deal with risk at the payments system level, and engaging issuers in the fraud mitigation process are critical. Important factors for success will be not only effectiveness in reducing CNP fraud, but also ease of merchant implementation and customer ease of use". – ***SmartCardAlliance.com***

paymentLOCK Message:

At paymentLOCK we have worked diligently to deliver a Card-Not-Present platform that delivers real-time merchant processing for any industry vertical in the US. A platform that creates flexibility and customization with world class security. Our goal is to empower every merchant with the ability to securely process CNP transactions anytime and anywhere through any web enabled device without compromising how you do business today. The above industry statistics and information clearly shows that CNP fraud will substantially rise in the US over the next 12-24 months. Taking the right security stance to protect your business will be key to eliminating your risk, brand reputation and fines associated to fraud. Be proactive. Protect your business and sensitive customer information by eliminating your exposure to CNP fraud today. Take the paymentLOCK Tour.

~ paymentLOCK Security Team ~

www.paymentLOCK.com

Aite Group, Card Fraud in the United States: The Case for Encryption, January 2012
http://www.emvco.com/documents/EMVCo_EMV_Deployment_Stats.pdf
The Nilson Report, Issue 1023 4 www.cybersource.com/US/Fraud-Report 5
http://www.fico.com/en/Company/News/Pages/10-10-2013-FICO-Data-Shows-the-US-Credit-Card-Fraud-IncidentRate-Rose-17-Percent-Over-Two-Years.aspx
Annual Report of the Observatory for Payment Card Security, 2011
https://www.pcisecuritystandards.org/