THE BUSINESS IMPACT OF CARD NOT PRESENT FRAUD

Jane Doe
Not Valid Unless Signed
present and future rules ... ations. If found, please return to:

Entrust Datacard™

+1-888-690-2424 | entrust.com

Table of Contents

Introduction to Today's Consumer

Today's consumer lives under the constant threat of identity theft, worrying that attackers will steal their money from their bank or credit card account. Depending on the liability policy in effect for a specific crime, anyone, consumer, retailer or bank alike, could be held accountable for the loss, which makes it a tough time to be in the payment card issuance or acceptance business.

United States' credit card fraud is now at 10 basis points, which is a 100 percent increase from just seven years ago. This increase is largely due to fraud at the point of sale (POS) as well as mounting card-not-present (CNP) fraud. CNP fraud, the unauthorized use of a payment card at any transaction where the cardholder does not physically present the card, is one of the security risk types that currently most threatens today's financial institutions, retailers, and businesses.

United States online and mobile commerce is growing at a 15 percent annual rate, which reinforces the importance for merchants to balance fraud prevention measures with the user experience.

Against this backdrop, the Europay, Mastercard and Visa Standard (EMV) arrives as a new variable in the fraud prevention landscape. The United States has joined more than 80 countries around the world in upgrading its payment card security to embrace EMV. The chip embedded in an EMV card creates a dynamic code that is unique to each transaction and significantly reduces the risk of counterfeit card use at the POS.

While reduced counterfeit fraud is good news for the issuers that have been enduring rapidly rising fraud rates, criminals are refusing to take the hit to their bottom line.

Every country that has adopted EMV has seen a precipitous increase in attacks of CNP fraud, and the United States will be no different.

Loss, Liability and the Impact of CNP Fraud

CNP fraud is on the rise globally—it currently represents about 45 percent of total United States card fraud. In a CNP attack, the attacker uses a copy of the consumer card number, expiry date and CVV to make an online purchase of goods.

The merchant unwittingly processes the fraudulent transaction because the attacker has gained access to the card's most sensitive information. Without physical handling of the payment card, there is not an opportunity to verify the cardholder's identity. The victim, who usually remains in possession of the compromised card, is typically unaware of the fraud until after the unauthorized activity has occurred.

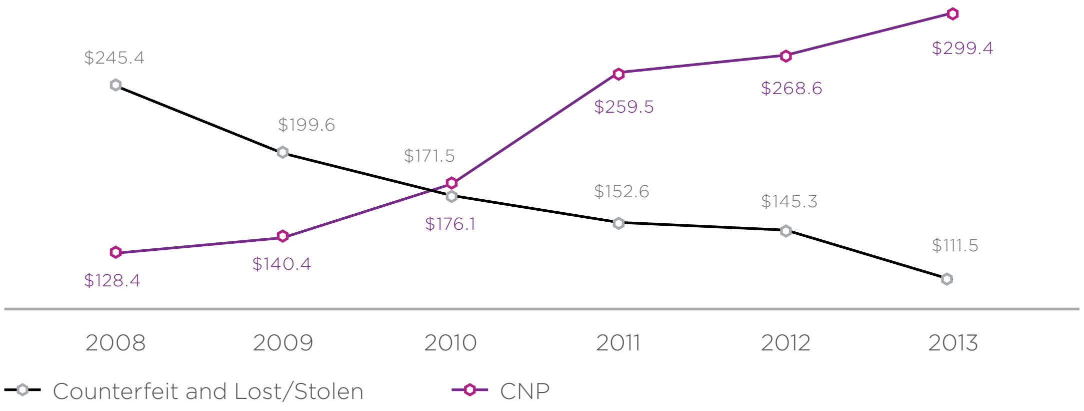
The information necessary to commit CNP fraud can be gained through a variety of methods including skimming, phishing and other carding methods. Unlike transactions in which a card is present, the loss liability for fraudulent CNP transactions falls to the merchant, which means the payment processor will charge the full value of the fraudulent purchase back to the merchant.

Countries that embrace EMV cards often see a dramatic rise in CNP fraud.

The chip-enabled EMV cards decrease counterfeit card fraud at Point of Sale (POS) and ATMs as attackers cannot counterfeit the card's magnetic stripe. However, the EMV chip is not utilized when making transactions at non-EMV-enabled locations—which includes certain POS terminals, and any online banking or shopping transaction—anywhere the card is not physically presented.

The estimated annual loss a financial institution operating with a legacy security system experiences from CNP Fraud is $1,040,000. The financial institution is responsible for 26 percent of the loss. The bulk of the responsibility, however, falls to the merchant.

CNP Fraud Puts trust In Digital Commerce at Risk

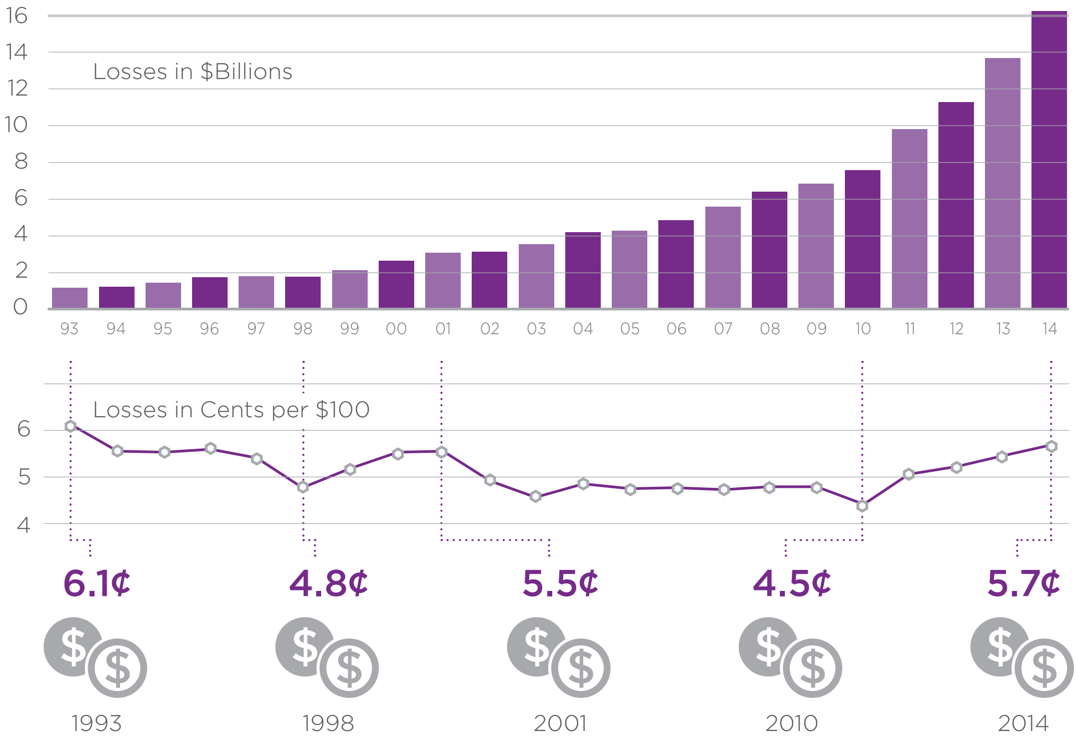


A financial institution running on newer technology, however, only experiences $500,000-$800,000 in losses. When the 26 percent is factored in, the bank saves roughly $200,000 - $500,000. With fraud costs continuing to rise at 19 percent per annum, there is a business case to be made for employing new technologies.

When CNP fraud does occur, the consumer whose information has been stolen will switch banks or stop using their EMV card altogether for online purchases until their confidence is restored. With the cost to acquire a new customer averaging at around $200, CNP fraud poses a great threat to all financial institutions.

The good news is that a number of technologies available to merchants and issuers - such as strong authentication, tokenization, behavioral analytics, and 3D Secure - have the potential to hamper the impact of future threats. A solution that helps secure online channels without placing huge demands on the consumer is what today's financial institutions need.

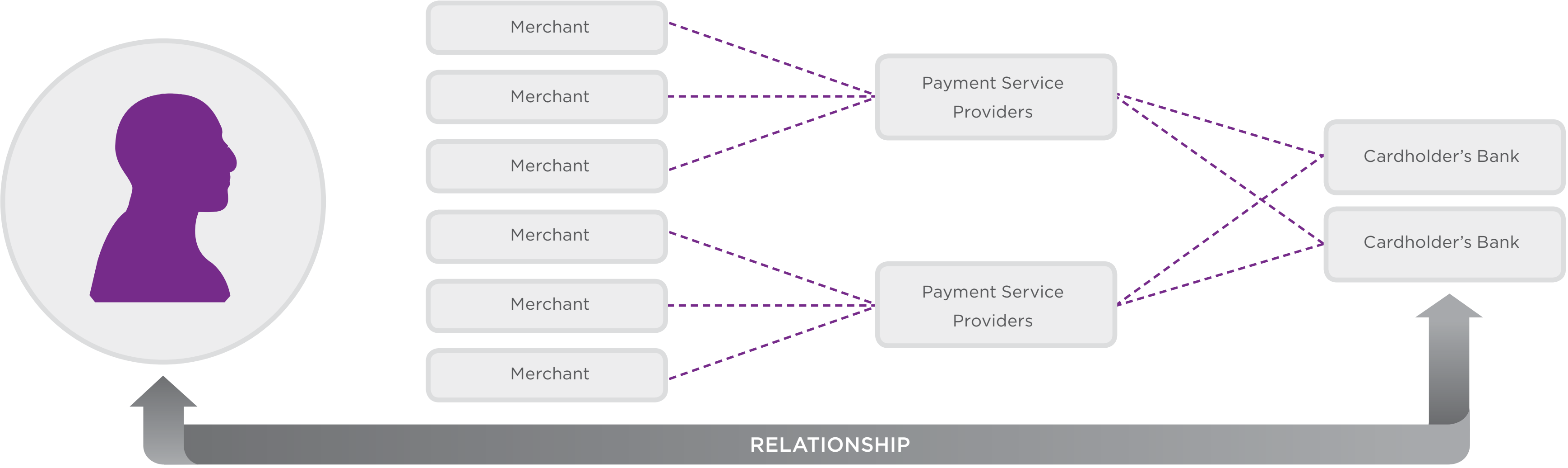
Card Fraud Worldwide



Overview of the Payment Network

The European Banking Authority's Security of Internet Payments guide allows for any of the three participants in the payment transaction shown in the diagram below to authenticate transactions. Some of the security challenges and solutions facing these participants are:

Figure 2 The Payment Transaction



Merchant: The merchant has an existing relationship with their consumers, which enables the merchant to request the transaction to be approved by the consumer through strong authentication. This will reduce the merchant's cost of fraud and improve consumer confidence in that merchant—leading to more purchases. From the consumer viewpoint, they will still experience fraudulent transactions as the counterfeit card will be used to make purchases in a country or merchant that does not require strong authentication. Another important consideration is that the consumer would require an authentication credential from each and every online merchant they deal with making it cumbersome to use and manage. Each merchant bears the additional cost of compliance, which is passed on to the consumer as higher prices.

Payment Service Providers (PSPs): The payment service providers do not have a direct relationship with the consumer. The merchant must share their consumer relationship with their PSP to allow for a common solution, where the transaction is sent to the consumer for approval by strong authentication. Care must be taken within a region to prevent the consumer from being inundated with disparate authentication schemes across several PSPs. This could be achieved by PSPs within a region sharing a common framework for consumer transaction approval.

Card Issuing Bank: On receipt of a payment request, the card issuing bank needs to implement transaction verification, so that regardless of where the transaction originates, it will always end up with the consumer for approval. The bank no longer needs to rely solely on complex fraud detection to look for purchase irregularities. This provides the best consumer experience since there is only one authentication credential required regardless of the online merchant.

A Better Approach to Securing Payments

There are many different approaches to securing e-commerce transactions.

What businesses must consider is how a secure approach might impact the integration and deployment complexity of a given solution.

Solutions for Securing Internet Payments

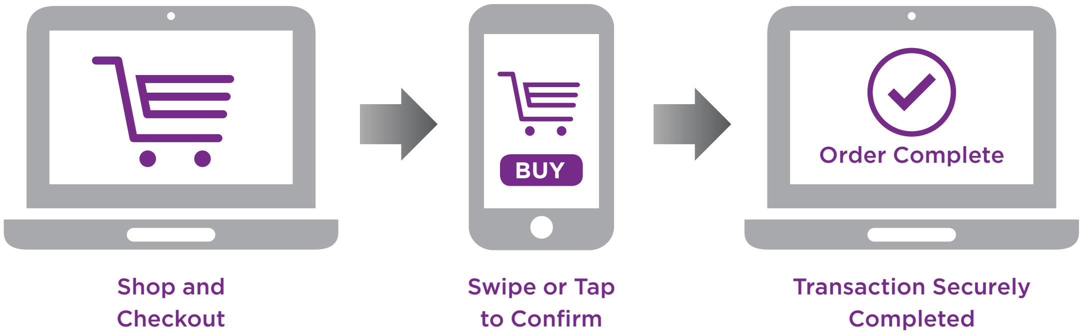
There is a broad range of solutions that are available to help secure Internet payments. Transaction Verification, Dynamic Card Verification Value and Adaptive Authentication all provide methods for authenticating transactions.

Real-Time Transaction Verification

A real-time transaction verification solution offers financial institution the best of all possible outcomes. Transaction verification works because it binds the digital identity to the cardholder, and often protects it, either through security and hardware inherent on every mobile device or via strong encryption. The right transaction verification solution will be built to ensure that every transaction gets completed every time.

When card issuing banks implement transaction verification, cardholders are protected regardless of where the purchase or payment originated. By implementing a transaction verification solution, financial institutions can increase control while simultaneously ensuring a positive customer experience, gaining the opportunity to introduce new services that can drive increased customer stickiness and revenue down the road.

Secure Payment



Dynamic Card Verification Value (dCVV)

Card Verification Value (CVV) codes, also known as CSC (card security code) or CVC (Card Verification Code), the three-or-four-digit code on the backside of credit and debit card are well-known features in card security. The standard CVV code is often used as a replacement for a PIN (personal identification number) during online transactions to prove the buyer is in possession of the card.

The CVV code alone, however, does not provide enough security. The CVV code has become susceptible to phishing and other identity stealing scams. Once the criminal is successful, they can make as many transactions as possible using the card's CVV details.

Dynamic Card Verification Value (dCVV) or Dynamic Card Verification Code (dCVC) technology is the most secure version of a CVV code. dCVV cards feature a mini-screen on the back of the credit card (where the CVV code is commonly displayed). With this authentication method, the 3-digit display of a one-time-password (OTP) value randomly changes every two minutes without the cardholders having to press a button or install any special plug-in on their internet browser. Thus, if the card's dCVV gets stolen, the data becomes useless in the next hour.

With dCVV, the consumer experience does not change. The card user still types in a 3 digit code—the difference is that neither the user nor a criminal can memorize the singular value. E-merchants do not have to modify their existing websites, and customers do not have to worry – as the merchant is not allowed by PCI policy to store the CVV. dCVV is fully transparent—implementation and use do not change.

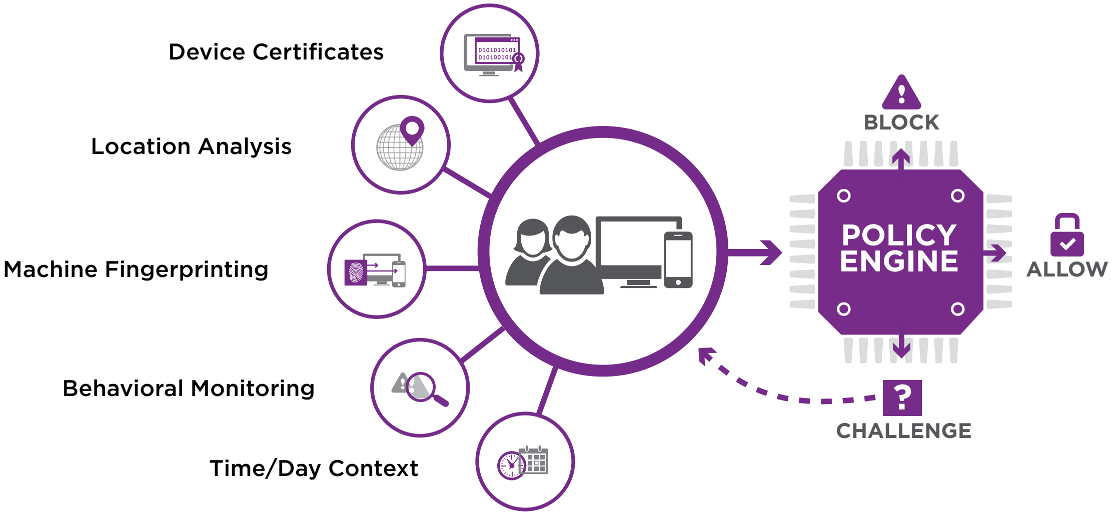
The most successful implementations of dCVV require a strong authentication solution integrated with the financial institution's payment system to create/delete the dCVV codes, as well as the use of a card printer/personalization system that can install the OTP seed value into the card's OTP chip over a contactless interface. The dCVV method is incredibly useful when paired with additional authentication methods.

Adaptive Authentication

Usernames and passwords are now insecure and frustrating to use, and strong authentication is necessary to keep information secure. Traditional authentication methods, however, get in the way of business. The resulting challenge becomes discovering how to implement controls that delight customers with their ease-of-use, but disappoint hackers thanks to top-level security. The solution to this problem is adaptive authentication.

Adaptive authentication works in real-time analyzing background information that helps financial institutions assess whether an online shopper is who they say they are. Adaptive authentication solutions use contextual data such as mobile and PC device fingerprinting, geolocation, velocity analysis, device certificates and even user behavior to build a real-time risk profile.

Each time the user is online his or her transactions are assessed for risk. If the risk is low, users are granted access to resources without having to perform a second factor of authentication. If the risk is high or the transaction is sensitive, an adaptive platform can challenge the user to authenticate. In extreme situations, users can even be denied access.



Adaptive authentication allows administrators to be more flexible and define policies tuned to the business or to specific user groups. Along with scoring and weighting parameters, information can be imported from 3rd party systems to provide a 360-degree view of users.

These capabilities allow administrators to design finely tuned security policies while reducing unnecessary step-up challenges, user friction and help desk support costs.

Conclusion

Today's environment varies by region. The deployment of mobile devices is limited in some areas while others are adopting next-generation payment schemes using digital signatures from each transaction. In order to fight CNP fraud and allow your customers to reap the true benefits of EMV, you need a vendor and a platform that is committed to transition your customer base from one generation to the next.

About Entrust Datacard

Consumers, citizens and employees increasingly expect anywhere-anytime experiences — whether they are making purchases, crossing borders, accessing e-gov services or logging onto corporate networks. Entrust Datacard offers the trusted identity and secure transaction technologies that make those experiences reliable and secure. Solutions range from the physical world of financial cards, passports and ID cards to the digital realm of authentication, certificates and secure communications. With more than 2,000 Entrust Datacard colleagues around the world, and a network of strong global partners, the company serves customers in 150 countries worldwide.

For more information about Entrust products and services, call **888-690-2424**, email **entrust@entrust.com** or visit **www.entrust.com**.

Headquarters
Entrust Datacard
1187 Park Place
Shakopee, MN 55379
USA

Twitter Facebook Youtube LinkedIn Google+ RSS

Entrust Datacard and Entrust are trademarks, registered trademarks and/or service marks of Entrust Datacard Corporation in the United States and/or other countries. Names and logos on sample cards are fictitious. Any similarity to actual names, trademarks or tradenames is coincidental. ©2016 Entrust Datacard Corporation. All rights reserved.

Entrust Datacard™