Why 3D Secure Is Primed for Ignition

ca technologies

Where There Is Opportunity, There Is Risk

eCommerce is growing at an unprecedented pace, with over a billion mobile customers driving demand. Right alongside there is growth in eCommerce fraud and pressure from alternative payments. To compete, you must capitalize on this opportunity and manage all types of fraud, while providing a frictionless customer experience.

1.4B
smartphones are used globally.[1]

eCommerce is worth **$1,713B** and growing.[2]

$2.9B in CNP fraud loss in 2014 and expected to double by 2018.[3]

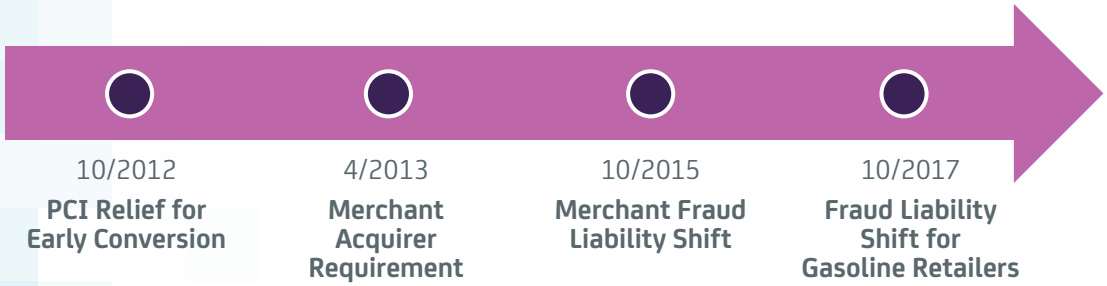
Alternative payments continues to grow, forecasted to own **59%** of all online transactions in 2017.[4]

1 Fierce Wireless, Report: Global Smartphone Penetration to Jump 25% in 2014, led by Asia-Pacific, June 11, 2014.
2 Taxamo, E-Services Boom Leading to E-Wallet Transactions Surge, March 10, 2014.
3 Payments Cards & Mobile, Alternative Payments to Overtake Credit and Debit Card Payments Globally, January 22, 2014.
4 Aite, Card-Not-Present Fraud in a Post-EMV Environment: Combating the Fraud Spike, June 2014.

Combating Card-Present Fraud

A few years ago, Visa announced its plan for a road map that would encourage all cards be transitioned from magnetic stripe technology to EMV chip-based technology. Then, similar plans were developed by MasterCard, Discover and American Express.

These road maps all clarify the timeline for the transition, as well as the penalties for parties that do not comply. For conversion of point-of-sale systems, all four major U.S. networks, as shown below address four common milestones: Effective October 1, 2015 is a counterfeit card liability shift, stating the party that has made investment in EMV deployment is protected from financial liability for card-present (CP) counterfeit fraud losses on this date. With the enforcement of this merchant fraud liability shift, millions of chip cards have been issued to U.S. consumers and millions of EMV-capable terminals and ATMS have been installed.



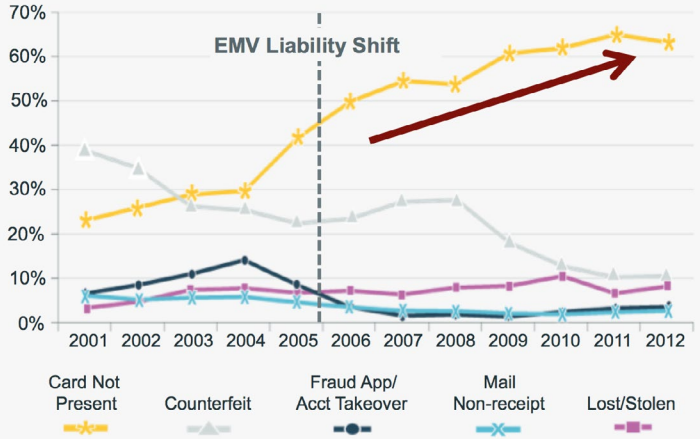
Post EMV Migration on Fraud Trends

Since the worldwide implementation of EMV, fraud losses from counterfeit cards have decreased by more than 63 percent. However, **card-not-present (CNP) fraud has increased dramatically**.

United Kingdom | Australia | France

63% growth rate

Almost immediately after banks in the United Kingdom began to ramp up EMV issuance in 2004, the country saw demonstrated success in reducing counterfeit card fraud, but an acceleration of fraud activity in the CNP category.



Based on these and other cases, there is a trend emerging that after a migration to chip-based cards there may be a decline in counterfeit and lost or stolen card fraud, but there will likely be a spike in CNP fraud as criminals seek new ways to exploit card accounts.

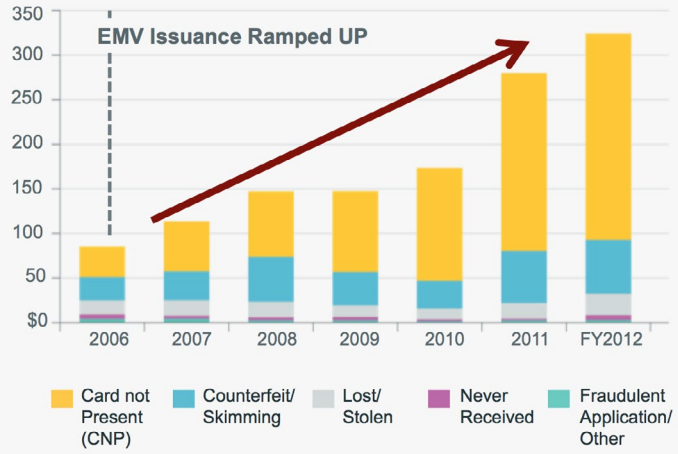
Post EMV Migration on Fraud Trends

Since the worldwide implementation of EMV, fraud losses from counterfeit cards have decreased by more than 63 percent. However, **card-not-present (CNP) fraud has increased dramatically**.

United Kingdom | Australia | France

39% growth rate

Card issuance in Australia was stimulated with interchange incentives for issuers, which began in 2004, when the original liability shift date of 2006 was put in place. So, while there was a high rate of quick adoption, CNP fraud grew at a compound annual growth rate (CAGR) of 39 percent.



Based on these and other cases, there is a trend emerging that after a migration to chip-based cards there may be a decline in counterfeit and lost or stolen card fraud, but there will likely be a spike in CNP fraud as criminals seek new ways to exploit card accounts.

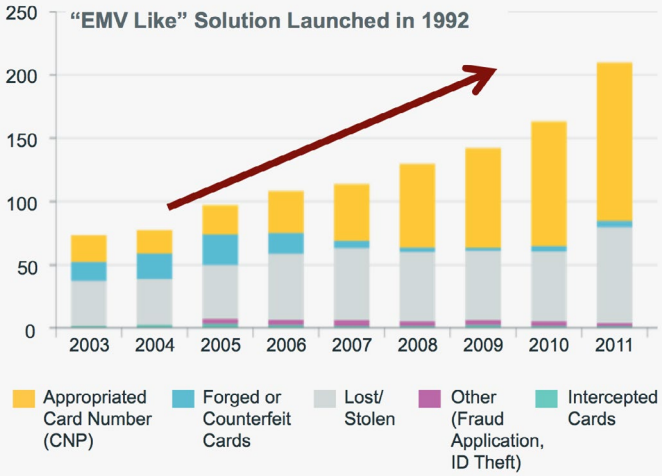
Post EMV Migration on Fraud Trends

Since the worldwide implementation of EMV, fraud losses from counterfeit cards have decreased by more than 63 percent. However, **card-not-present (CNP) fraud has increased dramatically**.

United Kingdom | Australia | France

25% growth rate

Having been the first national market to adopt chip cards for payments in the early 1990s, France has had a chance to adjust to evolving fraud trends. Even so, CNP fraud has grown nearly at a CAGR of 25 percent.



Based on these and other cases, there is a trend emerging that after a migration to chip-based cards there may be a decline in counterfeit and lost or stolen card fraud, but there will likely be a spike in CNP fraud as criminals seek new ways to exploit card accounts.

It's Time for Better Payment Security Online

By looking at the history of EMV migrations, it is clear that eCommerce fraud is a challenge that issuers cannot ignore. As more fraudsters move to the online channel because of the proliferation of EMV, and as overall volume in that channel continues its rapid expansion, the necessity for robust security and strategies for dealing with CNP risk will demand the attention of all parties in the payments value chain. Merchants, gateways, acquirer processors, etc.—all need to up their game when it comes to protecting online transaction data and invest in better solutions now.

Although all play a big role, issuers have one of the biggest opportunities to combat card-not-present fraud head-on.

Obstacles Facing 3D Secure Adoption

Some people still remember 3D Secure in its infancy. Although a very robust and effective solution from a security perspective, 3D Secure created too much friction in the checkout process and degraded the consumer experience due to a rather onerous registration process that was both time-consuming and confusing. This often would result in increased transaction abandonment, lost business for the merchant and lost interchange for the issuer.

The goal in the beginning was to improve security for online shopping and 3D Secure delivered. After the initial launch, the importance of creating an exceptional customer experience surfaced as an essential component of a viable payment security solution indicated by the level of merchant adoption with 3D Secure. Merchants would rather risk chargebacks than employ 3D Secure and risk losing the sale altogether. These obstacles made the new goal clear: issuers, merchants and cardholders expect online shopping to be easy and secure, so the objective is to strike the right balance.

How 3D Secure Is Exceeding Expectations Now

Today, 3D Secure has reached critical mass and continues to grow, offering a huge opportunity for issuers. 3D Secure is now much more sophisticated and provides the issuers with unique data about customer online shopping habits, such as device location, merchant URL, connection speed, etc.

By applying advanced analytics, **issuers can take advantage of this data** to:

Better identify fraud
while impacting
fewer transactions

Improve customer experience
and create value for issuers

Create customer insight
that helps issuers learn
more about the customer

In other words, by adding advanced analytics to the next generation of 3D Secure, issuers can gain the flexibility and control to make the most complex transactions frictionless, if desired.

So, how does it work?

The CA Technologies Multi-Layered Security Approach

Payment security solutions from CA Technologies help issuers overcome obstacles by offering zero-touch authentication to their cardholders. By migrating to a solution that employs a flexible and dynamic 3D Secure program and that utilizes neural network 3D Secure authentication models for continual risk-based assessment, issuers can more effectively combat eCommerce fraud without impacting the cardholder's online shopping experience.

In the scenario where a cardholder cannot be accurately identified, which results in a higher risk-score for that transaction, a convenient method of strong authentication can be used to accurately identify the cardholder in real-time. The combination of these three payment security solutions from CA Technologies can help issuers more successfully prevent ecommerce fraud, increase revenue, reduce card operations costs and improve the overall customer online shopping experience simultaneously.

Learn more about CA Security:

CA Transaction Manager	CA Risk Analytics	CA Strong Authentication for Payments

The CA Technologies Multi-Layered Security Approach

Payment security solutions from CA Technologies help issuers overcome obstacles by offering zero-touch authentication to their cardholders. By migrating to a solution that employs a flexible and dynamic 3D Secure program and that utilizes neural network 3D Secure authentication models for continual risk-based assessment, issuers can more effectively combat eCommerce fraud without impacting the cardholder's online shopping experience.

In the scenario where a cardholder cannot be accurately identified, which results in a higher risk-score for that transaction, a convenient method of strong authentication can be used to accurately identify the cardholder in real-time. The combination of these three payment security solutions from CA Technologies can help issuers more successfully prevent ecommerce fraud, increase revenue, reduce card operations costs and improve the overall customer online shopping experience simultaneously.

Learn more about CA Security:

CA Transaction Manager | **CA Risk Analytics** | **CA Strong Authentication for Payments**

CA Transaction Manager allows issuers to offer a flexible 3D Secure program to their cardholders. It enables full compliance with Verified by Visa, MasterCard SecureCode, JCB J/Secure, American Express SafeKey and Discover/Diners ProtectBuy cardholder authentication programs. It supports individual banks, global banks, service providers and processors who offer card management services. The flexible architecture facilitates integration with existing card issuer systems including home banking and fraud management systems and provides the foundation for adding advanced risk analytics to achieve zero-touch authentication.

The CA Technologies Multi-Layered Security Approach

Payment security solutions from CA Technologies help issuers overcome obstacles by offering zero-touch authentication to their cardholders. By migrating to a solution that employs a flexible and dynamic 3D Secure program and that utilizes neural network 3D Secure authentication models for continual risk-based assessment, issuers can more effectively combat eCommerce fraud without impacting the cardholder's online shopping experience.

In the scenario where a cardholder cannot be accurately identified, which results in a higher risk-score for that transaction, a convenient method of strong authentication can be used to accurately identify the cardholder in real-time. The combination of these three payment security solutions from CA Technologies can help issuers more successfully prevent ecommerce fraud, increase revenue, reduce card operations costs and improve the overall customer online shopping experience simultaneously.

Learn more about CA Security:

CA Transaction Manager | **CA Risk Analytics** | **CA Strong Authentication for Payments**

CA Risk Analytics transparently assesses the fraud risk of an ecommerce transaction in real-time during authentication. It accurately identifies legitimate transactions allowing the majority of cardholders to continue their purchase without impact. Using sophisticated advanced analytics, a behavioral neural network model and a flexible set of dynamic rules, it examines current and past transactions, device characteristics, location, user behavior and historical fraud data to evaluate risk. The calculated risk score is then used by your policies to decide whether to allow the purchase, request strong authentication, send an alert or deny the purchase. A comprehensive case management system allows immediate access to fraud data so that analysts and customer support representatives can prioritize and take action on cases, query fraud data and manage alerts.

The CA Technologies Multi-Layered Security Approach

Payment security solutions from CA Technologies help issuers overcome obstacles by offering zero-touch authentication to their cardholders. By migrating to a solution that employs a flexible and dynamic 3D Secure program and that utilizes neural network 3D Secure authentication models for continual risk-based assessment, issuers can more effectively combat eCommerce fraud without impacting the cardholder's online shopping experience.

In the scenario where a cardholder cannot be accurately identified, which results in a higher risk-score for that transaction, a convenient method of strong authentication can be used to accurately identify the cardholder in real-time. The combination of these three payment security solutions from CA Technologies can help issuers more successfully prevent ecommerce fraud, increase revenue, reduce card operations costs and improve the overall customer online shopping experience simultaneously.

Learn more about CA Security:

CA Transaction Manager | **CA Risk Analytics** | **CA Strong Authentication for Payments**

CA Strong Authentication for Payments is a cloud service that provides a wide range of authentication methods. It provides several mobile authentication options including push notifications, OTP via SMS/email and a mobile OTP app. Issuers have the freedom to choose whichever method of strong authentication they would like to employ, depending on what is necessary and practical for their cardholders.

The CA Technologies Advantage

Aside from the state-of-the-art technology, CA Technologies has experience in helping issuers dramatically reduce fraud in ecommerce transactions while keeping their cardholders happy with a pleasant online shopping experience.

- We literally co-wrote the book on the 3D Secure protocol to create an effective way to help payment fraud.
- We've been in operation since 2000; first branded as Arcot.
- The cloud service is hosted from SSAE-16 Type II SOC1 audited, secure and redundant data centers.
- We annually certify our compliance with Payment Card Industry (PCI) data security standards and the 3D Secure programs.
- Payment Security solutions from CA Technologies provide the best of both worlds: **significant fraud reduction** and a **frictionless customer experience** for the majority of legitimate cardholders.

To learn more about Payment Security solutions from CA Technologies, visit **ca.com/payment-security**.

To learn more about Payment Security solutions from CA Technologies, visit **ca.com/payment-security**.

CA Technologies (NASDAQ: CA) creates software that fuels transformation for companies and enables them to seize the opportunities of the application economy. Software is at the heart of every business, in every industry. From planning to development to management and security, CA is working with companies worldwide to change the way we live, transact and communicate – across mobile, private and public cloud, distributed and mainframe environments. Learn more at **ca.com**.

CS200-157384