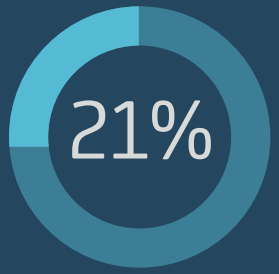
Reduce Friction and Decrease Abandonment for CNP Transactions With Payment Security From CA

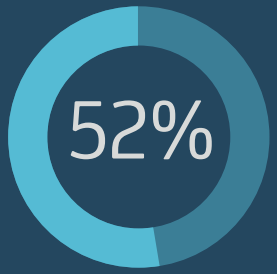
ca technologies

The Next E-Commerce Explosion

E-commerce sales are on the rise. Yet again.



DIGITAL SHOPPING INCREASE



MOBILE COMMERCE INCREASE

$142B PROJECTED SPEND

Consider Cyber Monday 2015: Digital spend during the annual online shopping holiday increased by 21 percent over the previous year—**surpassing the $3 billion mark** for the first time ever.[1]

Although desktop shoppers continue to drive this sharp rise in e-commerce spending, mobile devices have emerged as a prominent source of digital transactions. In fact, mobile commerce increased 52 percent on Cyber Monday 2015, rising to $838 million.[2] And, it's projected to account for $142 billion in spending by the end of 2016.[3]

All of this raises an important question:

How will our current fraud-prevention strategies cope with the substantial, continued growth of e-commerce transactions, especially when so many people now shop via their mobile devices?

1. "Cyber Monday Surpasses $3 Billion in Total Digital Sales to Rank as Heaviest U.S. Online Spending Day in History," comScore, December 2, 2015.
2. Ibid.
3. "US Mobile Phone And Tablet Commerce Forecast, 2015 to 2020," Forrester Research, 2015.

The Era of the False Positive

The answer is simple. Most existing fraud-prevention strategies aren't equipped to handle the marked increase in e-commerce—and in particular, mobile commerce—transactions.

Rather than help retailers and card issuers effectively prevent fraud, far too often these strategies end up creating an environment fraught with false positives—legitimate transactions wrongly declined due to suspected fraud.

While it may not be surprising, or even alarming, to see false positives increase in parallel with desktop and mobile commerce transactions, what's truly shocking is the amount of genuine business that's turned away as a result of these denials.

In 2014, declines based on **false positives totaled $118 billion**, with one-third of this figure coming from desktop and mobile commerce shoppers.[4] During that same time period, **$9 billion was lost due to actual card fraud**.[5]

The significant imbalance between false-positive declines and legitimate fraud is stunning—the **money lost to true fraud was 13 times less** than the total value of transactions terminated because of false positives.

Even so, global online fraud is set to top $25 billion by 2020, more than doubling current levels.[6] Though this is certainly a trend worthy of the attention it receives, the sheer volume of false-positive declines threatens to damage the consumer experience and the way shoppers interact with banks, card issuers and retailers.

2014: FALSE POSITIVES TOTALED

$118 BILLION

ONLINE FRAUD IS EXPECTED TO ECLIPSE

$25 BILLION BY 2020

4. "Future Proofing Card Authorization," Javelin, October 20, 2015.
5. Ibid.
6. "Online Payment Fraud: Key Vertical Strategies & Management 2016-2020," Juniper Research, March 5, 2016.

False Positives Drive Away Legitimate Business

False positives have become a significant nuisance for cardholders.

61%
DECREASED USING CARDS

Twenty-five percent of cardholders indicate they've experienced six or more declines on legitimate transactions in the past year.[7] And 61 percent of those cardholders say they've decreased using, or even completely given up on, a card after experiencing multiple false-positive declines.[8]

This poses a significant problem for issuers. Of course they want to eliminate fraud, but when the measures they employ force shoppers to abandon transactions after just a few frustrating declines—or even stop using their cards altogether—it can lead to some serious issues. It harms their brand reputations, prevents their cards from achieving "front of wallet" success and minimizes revenues gained from interchange fees.

Despite these risks, the majority of issuers still stick with the status quo: they continue to challenge transactions at a significant rate, forcing shoppers to suffer through multiple authentication exercises in order to complete just one order.

7. "Future Proofing Card Authorization," Javelin, October 20, 2015.
8. Ibid.

The New Way: Stop Fraud While Delivering a Frictionless E-Commerce Experience

Eliminating fraud remains a paramount concern in today's e-commerce environment. And rightfully so.

But the customer experience should be just as important. Online shoppers want their orders to be seamless. They want to fill their shopping carts, proceed to checkout and complete the order in the fewest clicks possible—no challenges or repeated questions aimed at verifying their identities and proving the transaction's legitimacy.

But as fraudsters become increasingly sophisticated, what's being used today will only become less and less effective—while remaining just as tiresome for genuine shoppers.

Because of this, issuers must become more flexible and able to change their fraud-prevention strategies at a moment's notice. And, crucially, they must do so in a way that matches customer expectations and makes the entire experience as easy and effortless as possible.

It's All About the Customer Experience

The customer experience now has a direct, decided impact on the payment ecosystem.

As a result, issuers must implement risk-based authentication practices that accurately verify customer identities without being overly intrusive. Doing so means eliminating static passwords and instead utilizing rich cardholder and device data to identify the risk of a payment transaction.

Recent announcements and regulations, such as 3D Secure 2.0 and the revised Payment Services Directive (PSD2), confirm the direction the CA Technologies Payment Security portfolio has followed over the last decade.

With a risk-based authentication solution powered by neural network models, issuers can transparently assess transactions in real time, making it possible to separate genuine orders from true fraud. Customizable rules and model thresholds support this approach, helping to set policies that allow or deny a purchase. And should a transaction exceed risk thresholds, issuers have the freedom to employ additional strong authentication methods as needed.

3D Secure 2.0 Is Coming

EMVCo, the body that manages security specifications for chip-based payment cards, recently **announced several advancements** to the 3D Secure protocol. For instance, 3D Secure 2.0 will request richer cardholder and device data during the transaction, which will result in far fewer password interruptions.

As a leading provider of 3D Secure solutions, CA Technologies is the ideal partner to help issuers migrate to 3D Secure 2.0. Our Payment Security solutions help prepare issuers for 3D Secure 2.0, while also supporting current 3D Secure protocols, enabling them to easily accept transactions from all merchants.

To learn more, read our **Viewpoint on 3D Secure 2.0.**

The Payment Security Solutions from CA Technologies

Payment Security solutions from CA Technologies help issuers achieve true zero-touch authentication. By migrating to a solution that employs a flexible and dynamic 3D Secure program—and utilizes neural network 3D Secure authentication models for continual behavior modeling and risk-based assessment techniques—issuers can more effectively combat fraud without negatively impacting cardholders.

With the Payment Security solutions from CA Technologies, issuers can successfully prevent fraud, increase revenue, reduce operational costs and improve the overall shopping experience.

Zero-touch authentication delivered:

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

With **CA Transaction Manager**, issuers can implement a flexible, comprehensive 3D Secure program that gives cardholders robust security, personalized one-to-one marketing and better customer service. Its flexible Software-as-a-Service (SaaS) architecture enables the solution to **easily integrate with issuers' existing systems**, including home banking and other fraud management systems, and freely support individual banks, institutions with multicountry operations and providers that offer card management services.

The Payment Security Solutions from CA Technologies

Payment Security solutions from CA Technologies help issuers achieve true zero-touch authentication. By migrating to a solution that employs a flexible and dynamic 3D Secure program—and utilizes neural network 3D Secure authentication models for continual behavior modeling and risk-based assessment techniques—issuers can more effectively combat fraud without negatively impacting cardholders.

With the Payment Security solutions from CA Technologies, issuers can successfully prevent fraud, increase revenue, reduce operational costs and improve the overall shopping experience.

Zero-touch authentication delivered:

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

With **CA Risk Analytics**, issuers can transparently assess the risk of a card-not-present 3D Secure transaction in real time by analyzing unique authentication data, such as device type, location, user behavior, historical trends and more. The solution utilizes patent-pending neural network authentication models that **facilitate zero-touch authentication** while simultaneously understanding what is normal for each individual cardholder. Issuers can support this approach with customizable rules and model thresholds, helping them set policies that allow or deny a purchase, as well as identify events that require additional authentication.

The Payment Security Solutions from CA Technologies

Payment Security solutions from CA Technologies help issuers achieve true zero-touch authentication. By migrating to a solution that employs a flexible and dynamic 3D Secure program—and utilizes neural network 3D Secure authentication models for continual behavior modeling and risk-based assessment techniques—issuers can more effectively combat fraud without negatively impacting cardholders.

With the Payment Security solutions from CA Technologies, issuers can successfully prevent fraud, increase revenue, reduce operational costs and improve the overall shopping experience.

Zero-touch authentication delivered:

CA Transaction Manager	CA Risk Analytics	CA Strong Authentication for Payments

With **CA Strong Authentication for Payments**, issuers can simplify transactions by offering **several mobile authentication options**—including push notifications and one-time passwords—all of which they can adapt with specific branding elements and other customizations. And because CA Strong Authentication for Payments generates one-time passwords for multiple accounts, it eliminates the need for cardholders to carry and manage multiple hardware tokens.

Striking the Right Balance Between Convenience and Security

With the help of the CA Payment Security portfolio, it's possible to deliver the experience customers demand. As a result, **issuers can**:

- **Gain and maintain "front of wallet" success** while increasing the frequency with which their cards are used.
- **Grow card revenue** by reducing the chances cardholders abandon transactions.
- **Reduce fraud losses**, minimize false positives and identify new types of fraud to support policy and rule creation.
- **Challenge only those transactions that appear truly fraudulent**, reducing the related costs.
- **Minimize the negative** financial and brand impact of fraud.
- **Reduce the time and expenses associated with operational, maintenance and implementation activities**, making it possible to reallocate resources to more strategic matters.

A Zero-Touch Authentication Case Study

A bank was struggling to enhance its fraud-prevention strategy while making the customer experience more streamlined and aligned with what today's cardholders expect.

With help from our robust Payment Security portfolio, as well as support from the Payment Security team, the bank updated its strategy—which previously saw them challenging nearly every transaction—to an intelligent, risk-based approach. Now, they're **approving 90 percent of transactions without a challenge**, making it far easier and less of a hassle for shoppers to complete their orders.

By enabling the bank to implement this new approach, our Payment Security portfolio made a **significant impact** on the customer experience—one that saw:

80%

REDUCTION IN ABANDONED TRANSACTIONS

50%

REDUCTION IN FAILED TRANSACTIONS

0%

NEGATIVE IMPACT FROM FRAUD

To learn more about the Payment Security portfolio from CA Technologies, please 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.

CS200-199719

ca technologies