Solution Brief

A Broadcom Company

Payment Security Suite

Fight Fraud and Keep Cardholders Spending with Data Science

Challenge

Card-not-present (CNP) fraud costs issuers billions of dollars in chargebacks and disputes. As eCommerce and mCommerce continue to grow, you need the right tools to fight back. And you need security that doesn't get in the way of genuine online transactions. In other words, you want to minimize fraud, avoid false declines and keep cardholders happy.

Opportunity

CA Technologies, a Broadcom Company, provides the path to reducing fraud while creating a smooth cardholder experience. Our unique global fraud risk network and industry-leading data science enables highly accurate decision-making. And our patented predictive analytics and machine learning capabilities leverage extensive and diverse data provided through EMV 3-D Secure (EMV 3DS).

Benefits

With Payment Security Suite, there's no need to compromise. You can reduce fraud and false declines while enabling a frictionless cardholder experience. You stay in control, maintaining your own fraud policies and systems while gaining the combined power of a flexible 3DS implementation, a dynamic field-programmable rules engine, and predictive neural network authentication models. Payment Security Suite enables you to take a big step forward in lowering your costs and motivating customers to choose your card over others.

Optimizing your cardholders' eCommerce experience keeps you top-of-wallet—both leather and digital. But streamlining checkout needs to be balanced with reducing card-not-present fraud. Now you can benefit from lower abandonment rates, reduced costs and increased revenue with one powerful solution.

Finding the Balance

Card-not-present (CNP) fraud has become so advanced that legitimate transactions can look deceptive and illicit ones can appear authentic. It's a thriving "industry" where perpetrators use readily accessible technology to constantly adapt to the security methods and practices designed to thwart them. These dynamics make it far more challenging than ever before for issuers to balance fraud mitigation with a frictionless cardholder experience.

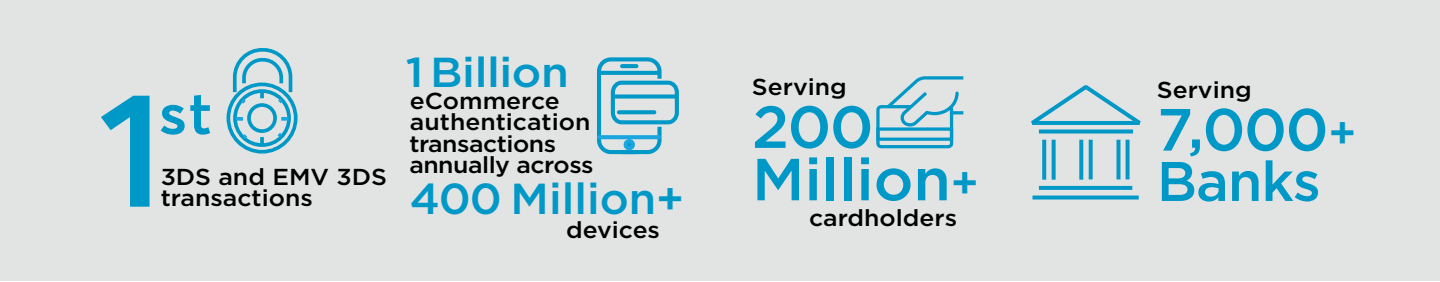
Your cardholders worry about the safety of their hard-earned money. Yet, when it comes to their online transactions, they want a smooth shopping experience without annoying authentication requests.

You're looking for an innovative approach to fraud prevention. One that provides a robust means of authentication across portfolios, channels, lines-of-business and geographies. And the flexibility to adapt to your business rules in real time, as well as the ability to combat crucial events, like flash fraud.

Payment Security Suite combines CA leadership in EMV 3-D Secure with real-time fraud risk learning and scoring derived from billions of eCommerce authentication transactions and world-class data models.

Our patented predictive analytics give you the insights you need to reduce losses as well as false declines. And it is the only solution that delivers true, real-time analysis—in mere milliseconds.

Figure 1. CA leads the way in fraud prevention.



Leading the Way in Fighting CNP Fraud

CA Technologies has been helping processors and issuers address payment fraud for nearly 20 years. Our uncompromising focus on the payments ecosystem has resulted in the largest global consortium network of fraud data.

With CA's investments in data science, we lead the way with industry-leading modeling—leveraging the vast number of transactions that flow through our payment security platform.

The numbers speak for themselves.

Cutting-Edge Fraud Protection

Payment Security Suite is a flexible SaaS solution that seamlessly integrates into your existing fraud prevention systems. With thousands of implementations worldwide, the solution has proven reliability, scalability and security.

Benefits include:

- Open and uncomplicated integration to support existing card issuer systems
- The ability to use a variety of authentication methods such as push notification, SMS via OTP and others
- The options you need to support banks with multi-country operations, service providers and processors offering card management services
- The flexibility to maintain separate silos and business rules for different card portfolios—applying policy even at the sub-BIN level
- Full compliance with all major card 3DS programs

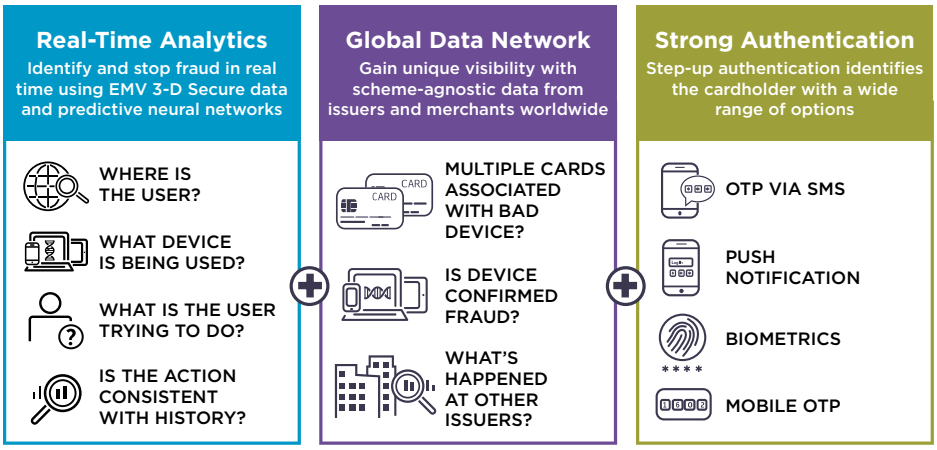
Payment Security Suite provides flexible authentication that enables issuers to seamlessly implement a custom and comprehensive EMV 3DS program. You have full visibility and control over all CNP transactions, reducing both fraud and false declines. This provides you with the best of both worlds. A set-it-and-forget-it payment security solution that you can change if needed—in real time and based on your business rules.

The solution is highly configurable, making it simple to achieve your branding, user experience, card portfolio and security requirements—down to the card level. A field-programmable rules engine allows you to dynamically create and manage business rules at the portfolio level.

Analytics Powered by Market-Leading Data Science

Payment Security Suite uniquely taps into the comprehensive network of cardholder transaction data—both recent and historical—across issuers and merchants. These analytics use neural networks and machine learning to gain insights from, and adapt to, fraud patterns in real time. It is this instant analysis of multi-dimensional, large-scale data that enables the transparent fraud assessment of eCommerce transactions.

Figure 2. Payment Security Suite combines real-time analytics, leveraging the CA global network of consortium data and strong authentication.



Predictive neural network authentication models are powered by advanced machine learning techniques that leverage data from EMV 3DS and the CA data network. These models enable accurate assessments in real time, discerning between legitimate and fraudulent transactions.

We maintain and analyze a vast amount of transaction data such as device characteristics, IP address, geolocation, transaction amount and much more. This provides the advantage of understanding a transaction in the context of what is normal for each individual device and cardholder.

Payment Security Suite employs a self-learning scoring model, which analyzes and compares historical and real-time transaction behavior. Card and device profiles are then immediately updated, influencing the model to reflect the most current and accurate risk score.

The system continues to learn from every purchase transaction in real time. This modeling is done across the consortium of both issuers and merchants, which yields benchmarks, comparisons and a richer data set upon which to generate the risk score. The evaluation of every transaction is a little smarter than the last, as the data set becomes richer and more tailored.

In the end, this analysis is designed to minimize the number of transactions deemed as risky and reduce the number of transactions that require step-up authentication.

Because fraud often occurs from the same or similar batch of bad devices, over a short time period with many cards, issuers often don't see this activity until well after the fact. To avoid accepting illegitimate transactions, you need behavioral information about a card and/or device in real time.

The platform adapts to fraud patterns in real time by leveraging this transaction intelligence and data across the global network. Its multidimensional view of transaction behavior analyzes and compares connections among card and device activities as they happen across banks, merchants and geographies. Payment Security Suite enables highly accurate decision-making via a combination of our unique global risk network and our in-house, industry-leading data science team.

Leveraging the real-time consortium network has been proven to result in a 25% savings in fraud losses and 35% reduction in false positives compared to single-issuer data.[1]

1 Data based on applying the CA Risk Analytics Network fraud model to historical customer data over a 90-day period.

When We Say Real Time, We Mean Real Time

Some providers say "real time" but, in truth they may be using models based only on confirmed historical fraud. And instead of accurately predicting fraud before it happens, they're essentially chasing after it.

At CA, real time means just that. With Payment Security Suite, a score arrives during the transaction, not after—and used automatically—so you can take action to avoid fraud before it happens.

When it comes to major fraud events, it's all about quickly recognizing the first fraudulent transaction to avoid the second, the third and so on. This can happen only with sophisticated machine learning.

In one half of all CNP fraud schemes, the second transaction occurs within 3.6 minutes of the first, and in 15% of these cases, it's less than one second. Compare this to an average of 5 days between legitimate transactions.

To achieve real-time protection, you don't need to take any special action—Payment Security Suite has you covered.

Figure 3. Figures are based on issuer usage of CA payment security solutions and 3DS 1.x data.

Risk-Based and Strong Authentication Working Together

Today's online shoppers are well aware of their exposure to data breaches and payment fraud. When it comes to security, consumers need confidence in their issuer. At the same time, they want an uninterrupted and hassle-free transaction experience.

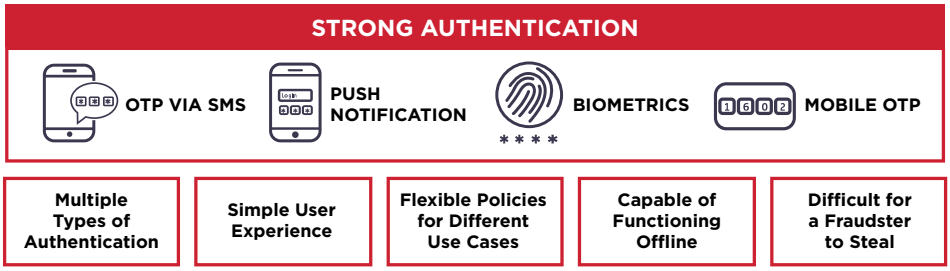
Payment Security Suite helps you know if and when step-up authentication should be introduced. This means the majority of transactions proceed without interruption. Your legitimate cardholders don't have to deal with the hassle of multiple authentication steps, and the fraudsters are more likely to be rejected.

You have the flexibility and freedom to set your desired fraud thresholds based on portfolio needs. For example, an issuer can prioritize customer experience by setting thresholds so that 95% of transactions go through unchallenged. The remaining 5% are either challenged with a secondary authentication request or flat out denied.

For the small percentage of transactions that must be challenged, a variety of authentication methods, including OTPs, push notifications and biometrics are available—enabling advanced authentication that is both flexible and scalable.

Multi-factor authentication not only reduces fraud risks, it is also necessary to comply with governmental regulations such as the European Banking Authority's Payment Services Directive (PSD2).

Figure 4. Payment Security Suite enables a variety of authentication methods.



EMV 3-D Secure Puts You in the Drivers Seat

EMV 3-D Secure (EMV 3DS) enables both issuers and merchants to fight CNP fraud. 3DS was co-invented by CA Technologies (then Arcot) and Visa in the early 2000s to protect against fraudulent eCommerce transactions. Now, the protocol has transformed into EMV 3-D Secure, sometimes referred to as 3-D Secure 2.0 (3DS 2.0).

The industry standard EMV 3DS was defined by EMVCo, a consortium of banks, merchants and payment organizations. As a Technical Associate of EMVCo, CA Technologies plays a key role in the process, contributing significant technical and marketplace expertise.

Today's EMV 3DS includes major improvements over the original version. Two significant ones—no requirements for static password nor initial sign-up process—create a much smoother eCommerce experience for cardholders.

The vast amount of valuable data that is available with EMV 3DS can play a pivotal role in your authentication strategy—greatly reducing the number of transactions challenged. And by supporting a wider range of devices, EMV 3DS payments can run in both in-app and browser-based solutions, for a consistent look and feel across all merchant interfaces.

The financial benefits of EMV 3DS for issuers go well beyond fraud protection. With fewer occurrences of fraudulent transactions, a reduction in challenges and more true sales, you can reduce the operational costs associated with CNP fraud.

Plus, more legitimate sales and a better shopping experience for cardholders result in further confidence in your products—keeping them top-of-wallet. A variety of tools enable you to extract EMV 3DS-generated data to analyze cardholder buying behaviors. With this information, you can design new products and services that create a more seamless and unified commerce experience.

Figure 5. One bank's experience with Payment Security Suite

THE CHALLENGE

For a major European bank, first-rate customer experience is the name of the game, but:

- It had an overly cautious, one-size-fits-all approach to CNP transactions.
- While fraudsters were becoming more sophisticated, cardholders were suffering more delays.
- Delays were turning into missed opportunities—for the bank and its cardholders.
- Finding the right balance between fraud protection and frictionless customer experience was priority one.

THE SOLUTION

With Payment Security Suite, the bank now has:

- Trust in its risk scores.
- Confidence that the right transactions will go through without interruption.
- The ability to set challenge parameters that make sense for its business.
- A reduction in password challenges, from 100% down to 15-20%.
- Enhanced data insight that has led to reduced fraud losses and improved customer experience.

NEXT UP: IDENTITY RISK INSIGHT SUITE

Identity authentication across the enterprise:

- Customers expect a secure, unified experience for all their banking and financial needs.
- The bank benefits from one identity authentication solution for all of its digital financial services.
- With Identity Risk Insight Suite, the bank safeguards customers with predictive neural network monitoring.
- Customers are protected from identity fraud across online, mobile, lending, insurance and other banking services.
- Now the bank can deliver a consistently positive digital experience across products and channels.

Identity Risk Insight Suite—Authentication Across the Enterprise

Global digital businesses are prioritizing mobile-first strategies that cater to the needs of a growing, tech-savvy customer base—one that demands frictionless access to online goods and services. Yet the threat of cybercrime looms large as fraudsters trade stolen identity data to perpetrate global attacks.

Identity Risk Insight Suite (IRIS) enables banks to deploy the state-of-the-art capabilities available in CA's payment security solutions across their entire enterprise. IRIS supports other applications, including online banking, mortgage, insurance, lending and more.

With a single cross-channel fraud prevention solution, you can take advantage of our patented predictive analytics to share data across digital financial services offerings. This means you can protect other online channels, gain cross-channel visibility and implement an omnichannel authentication experience for your customers.

IRIS gives you the ability to genuinely recognize good, returning customers by piecing together their digital identity from the complex digital DNA users create as they transact online. High-risk behavior can be pinpointed in real time, whether at new account applications, logins or payments, reducing friction and unnecessary step-ups.

IRIS extends our proven predictive modeling and risk analytics capabilities—currently applied to the highly regulated payments space—across the enterprise to drive out fraud on all digital channels and satisfy industry mandates. IRIS enables you to deliver a consistently positive digital customer experience across products and channels. It provides a robust data set by synthesizing different types of anonymized interaction information. While profiles represent a specific individual, the individual remains anonymous.

Solution Brief

Summary

With Payment Security Suite, you're in control. You can set the risk policy and authentication experience for your cardholders via your own risk structure, rule-building tools and existing fraud systems. Payment Security Suite is flexible, which means that you can integrate the platform with your current systems and policies. And it provides robust means of authentication across portfolios, channels, lines-of-business, and geographies. In the end, Payment Security Suite enables you to stay top-of-wallet.