Laying the Foundation for Better Intelligence with EMV® 3-D Secure

How merchants can use richer data to combat fraud and gain a competitive advantage
E-commerce continues to accelerate, with Forrester reporting a 16% year-over-year increase in online retail sales in 2018. But that growth has a darker side: online or card-not-present (CNP) fraud is accelerating even faster. And CNP fraud now accounts for 81% of total fraud losses.

Issuers have implemented a variety of authentication tools to combat CNP fraud but some of these tools are sub-optimal. Often, they rely on a guilty-until-proven-innocent authentication model that requires legitimate customers to jump through hoops to prove that they are who they say they are. Good customers are asked to enter hard-to-remember login credentials or answer intrusive knowledge-based authentication (KBA) questions.

When this happens, genuine customers are required to painstakingly undergo numerous authentication requests. Frustrated by the friction in their online shopping experience, a majority of customers will choose to abandon the transaction altogether.

---

**False declines will exceed $330B in the U.S. in 2018...**

E-commerce continues to accelerate, with Forrester reporting a 16% year-over-year increase in online retail sales in 2018. But that growth has a darker side: online or card-not-present (CNP) fraud is accelerating even faster. And CNP fraud now accounts for 81% of total fraud losses.

Issuers have implemented a variety of authentication tools to combat CNP fraud but some of these tools are sub-optimal. Often, they rely on a guilty-until-proven-innocent authentication model that requires legitimate customers to jump through hoops to prove that they are who they say they are. Good customers are asked to enter hard-to-remember login credentials or answer intrusive knowledge-based authentication (KBA) questions.

When this happens, genuine customers are required to painstakingly undergo numerous authentication requests. Frustrated by the friction in their online shopping experience, a majority of customers will choose to abandon the transaction altogether.

---

**Harms customers**

- **58%** feel frustrated when a credit or debit transaction is declined due to suspicion of fraud
- **33%** want security mechanisms to be behind-the-scenes

**Harms merchants**

Average decline rate for CNP transactions:

- **20%** vs. **3%** for point-of-sale transactions

---

2. Aite Group survey of 1,400 consumers in the U.S., July 2018
4. Aite Group survey of 1,400 consumers in the U.S., July 2018
In an online survey conducted by Aite Group, consumers were asked how they feel when a credit or debit card transaction is declined because of suspicion of fraud. Not surprisingly, the majority of consumers—58%—feel very or slightly frustrated.2

In addition to customer friction, many fraud detection tools can return a significant number of false declines—which has an enormous impact on merchants’ revenue and their relationships with their customers. Indeed, false declines will exceed $330 billion in 2018 in the U.S. market alone, estimates Aite Group.3 The CNP channel is disproportionately affected by false declines, with the average decline rate for a CNP transaction between 15% to 20% versus 2% to 3% for card-present transactions.

Customers don’t mind security per se—they want to shop safely and securely—but they don’t want to be hassled with difficult, time consuming authentication requests. Aite Group asked consumers how they viewed security mechanisms: one-third said they prefer security mechanisms to be behind-the-scenes as much as possible, so they have little or nothing to do to authenticate themselves.4

The Promise of EMV® 3-D Secure

One of the most promising advancements in the fraud detection arsenal is EMV® 3-D Secure (EMV 3DS), an industry standard protocol that is designed to make online shopping transactions frictionless and secure by specifying the data for authenticating cardholders. EMV 3DS was recently finalized by EMVCo, the global body that manages the chip card specification. Beginning in 2019, EMV 3DS will be used by all card scheme brands including Mastercard Identity Check, Verified by Visa, American Express SafeKey®, and Discover ProtectBuy.

EMV 3DS creates a data connection between merchants, payment networks, and financial institutions in order to analyze up to 150 data elements and share more intelligence about transactions. With this protocol in place, these stakeholders can fully collaborate with each other to combat fraud and return better risk decisions to merchants.

EMV 3DS provides the authentication points needed to reduce fraud rates, false declines, and abandoned shopping carts as well as setting the foundation for innovative companies to combine data science, dynamic rules engines, market insights, and more.
The protocol also supports both browser-based and mobile app-based purchases and provides a unified web and mobile experience, critical since more than one-third (35%) of successful fraudulent transactions among large merchants occur on the mobile channel.

Building on the EMV 3DS Foundation

While distinguishing good transactions from bad and mitigating fraud is the overriding goal of upgrading to EMV 3DS, it’s also important that transactions are still allowed to happen at lightning speed, with a good shopping experience. EMV 3DS allows providers like CA Technologies, a Broadcom Company, to utilize data from merchants, payment networks, and financial institutions around the globe to provide a 360 degree view of transactions. Third parties can then add their own data to the already robust set of data elements in EMV 3DS to drive better insights and decisioning.

For nearly 20 years, CA has led the way in authentication and fraud prevention. As the world’s largest 3DS provider, CA was first to deploy 3DS and the first to authenticate an EMV 3DS transaction—delivering state-of-the art protection and a seamless customer experience. CA’s patented fraud analytics give issuers, processors, and merchants the real-time insights they need to reduce false declines and increase conversions.
CA’s neural network models learn from the relationships between the data elements, improving decision making even further over time. The models also adapt to changing fraud patterns, giving merchants a more confident risk-based assessment of fraud patterns in real time, to allow, deny, or offer up a secondary authentication method for a given transaction.

CA also enables merchants to configure and manage authentication based on their own risk policies and risk tolerance. Merchants can rely on the issuer’s decision—which shifts liability to the issuer—or use EMV 3DS in non-challenge mode, giving them ultimate say over whether or not to approve a transaction.

**Why CA Technologies?**

To unlock the ultimate value EMV 3DS possesses, merchants will need to partner with a leader in both 3-D Secure & data science. As the co-inventor of the original 3-D Secure protocol, CA (then Arcot) has deep expertise in the protocol. Today, CA is a Technical Associate member of EVMCo and one of the main contributors to the EMV 3DS standard.

With its experience, CA has assembled the largest global network of EMV 3DS e-commerce authentication transaction data. This network handles one billion e-commerce authentications across more than 400 million devices annually. CA serves 7,000 financial institutions and protects 200 million cardholders around the world.

Since its early days as Arcot, the company has invested heavily in data science resources and has the ability to extract intelligence from complex data sets that provide unsurpassed visibility into transactions providing the greatest to issuers and merchants.

**EMV® 3-D Secure + CA Technologies = More value for merchants**

CA Technologies helps merchants combat fraud and lay the groundwork for even greater business insight.
Fighting Fraud with Intelligence

The rich data analytics supplied by CA enables highly accurate authentication decisions, which means the vast majority of shopper transactions going through unchallenged. For consumers, this means a frictionless checkout. For merchants, this means fewer false declines and a reduction in chargeback liability.

But merchants can gain even more from EMV 3DS. With the right partner, merchants can use this wealth of data in new and innovative ways that not only reduce fraud but provide customer intelligence to inform the development and improvement of delivery channels, products and services, and the customer experience.

About CA Technologies

CA Technologies, a Broadcom Company, is the industry leader in payment and identity fraud prevention, with friction-free transaction authentication powered by patented artificial intelligence. As the world’s largest 3-D Secure provider and a pioneer in data analytics for online fraud—powered by the largest global data analytics network in the industry—CA delivers a unique 360° view of transactions for issuers, processors and merchants, across all payment schemes. Learn more at ca.com/merchants.