Aite PARTNER. ADVISOR. CATALYST.

3-D Secure: The Force for CNP Fraud Prevention Awakens

Prepared for:

RSA®

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

INTRODUCTION

Card-not-present (CNP) fraud is on the rise across the globe, fueled by a perfect storm. E-commerce is growing at a rapid clip, outpacing physical store sales in many areas. Chip cards are replacing the ineffective mag stripe in countries around the world, making counterfeit card fraud much more difficult to perpetrate and prompting a migration to CNP fraud. At the same time, data breaches are rampant, providing criminals with a robust supply of stolen card data.

Merchants and issuers alike are increasingly looking to add 3-D Secure (3DS) to their CNP fraud-prevention toolkits. Merchants are driven by the desire to stem rising fraud losses, while issuers are motivated by a desire to rein in fraud and also maintain consumer confidence in the security of online transactions. While 3DS stumbled out of the gates in its original incarnation, significant changes to the protocol have been realized in the ensuing years to make it much more user friendly.

This white paper provides an overview of the current CNP threat environment and discusses 3DS' progression from a clunky attrition machine to a valued tool in merchants' and issuers' fraud-mitigation arsenals.

METHODOLOGY

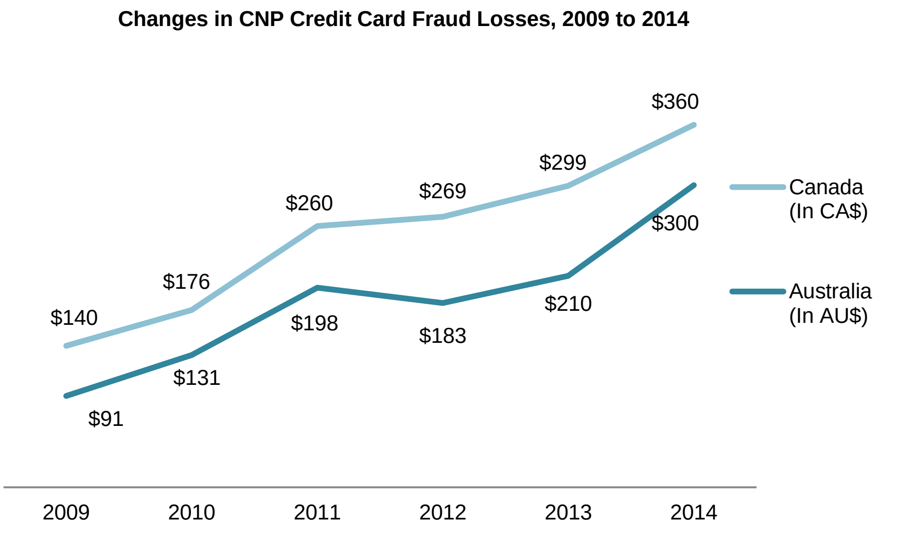
Aite Group interviewed 31 executives from global merchants, issuers, payment networks, processors, and 3DS vendors from November to December 2015 to understand the industry's current and planned use of the 3DS protocol.

THE RISING TIDE OF CNP FRAUD

The good thing about being the last G-20 country to migrate to EMV is that there are plenty of examples that payments executives in the United States can learn from. A key lesson from preceding EMV migrations is that as a country moves to chip cards, fraudsters shift tactics. A key area of increased criminal focus is CNP fraud. As it becomes increasingly difficult to buy stolen card data and turn it into counterfeit cards, fraudsters instead use compromised card data and credentials to perpetrate e-commerce fraud.

Australia and Canada provide good examples of the migration of fraud from the point-of-sale (POS) to CNP. Australia's liability shift took place in April 2012 for MasterCard, and April 2013 for Visa. Australia's e-commerce fraud losses increased 30% from 2013 to 2014, while its aggregate e-commerce sales growth was only 9% for the same period.[1] Canada's credit card liability shift took place in April 2011, and it saw a 38% increase in CNP fraud over the next three years (Figure 1).

Figure 1: Australian and Canadian CNP Fraud



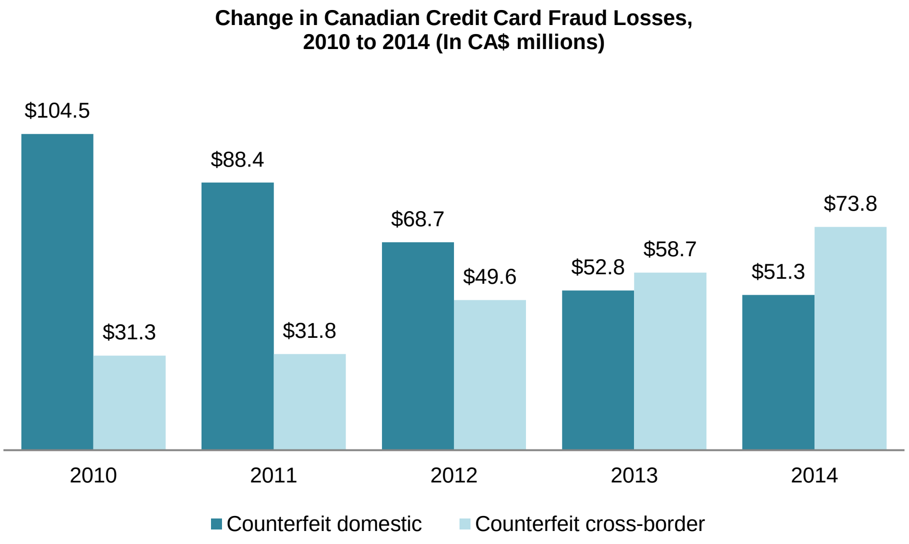
Source: Australian Payment Clearing Association, Canadian Bankers Association

As all countries have migrated to EMV, cross-border counterfeit card fraud has been a notable outlet for stolen card data. Canada's experience exemplifies this; domestic counterfeit fraud decreased since the introduction of EMV, while cross-border counterfeit fraud rose steadily as criminals took stolen card data south of the border and perpetrated counterfeit card fraud in the mag-stripe-dependent United States (Figure 2). As the United States moves to EMV, there is no

[1] NAB Online Retail Sales Index, accessed on January 12, 2016, http://business.nab.com.au/wp-content/uploads/2015/03/NAB-Online-Retail-Sales-Index_in-depth-report-January-20151.pdf.

other card market of a sufficient size and scale to serve as an outlet for cross-border fraud, which will result in increased pressure on CNP.

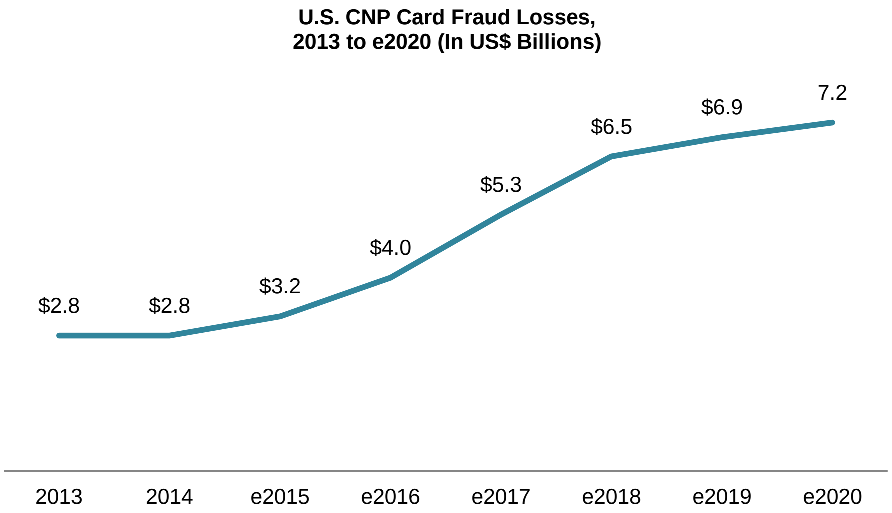
Figure 2: Canadian Domestic and Cross-Border Counterfeit Fraud



Source: Canadian Bankers Association

With the converging pressures—data breaches, the U.S. EMV migration, growing e-commerce volume—a painfully sharp rise in CNP fraud as the United States migrates to EMV is not outside the realm of possibility. Aite Group believes that the rise will be felt—indeed, Aite Group's interviews with U.S. issuers and merchants indicate that the criminals didn't wait for the October 1 liability shift date to increase their attacks on the CNP environment. The spike will be less impactful than circumstances would suggest, however, due to the industry's increased adoption of technologies such as tokenization, behavioral analytics, and 3DS (Figure 3).

Figure 3: Current and Projected U.S. CNP Fraud



Source: Aite Group

RISK-BASED 3-D SECURE: THE FORCE AWAKENS

Many issuers and merchants still cringe when they hear the term “3-D Secure,” as they envision 3DS’ painful first iteration, which featured a clunky user experience and cart abandonment. The payment networks and vendors have made substantial improvements to the protocol and its enabling solutions since this awkward adolescent phase, however, and merchants and issuers alike are increasingly giving 3DS a second chance.

3DS is designed to bring additional layers of authentication to CNP transactions. If a merchant invokes 3DS, then it will benefit from a liability shift back to the issuer if the transaction is fraudulent. The first version of 3DS was pretty much an all-or-nothing proposition from the merchant’s perspective. It could either send all of its transactions across the 3DS rails or none of them. That’s a thing of the past, as many merchant plug-in providers now enable merchants to selectively decide which transactions they would like to send.

3DS also initially relied on static passwords, which were infrequently used by the consumer and quickly forgotten. With the first iteration, stepped-up authentication was invoked for every transaction. All of this, combined with the use of confusing pop-up boxes, understandably resulted in substantial customer attrition. The technology has come a long way since then, and the market is rapidly moving to risk-based authentication (RBA) and dynamic stepped-up technology. The risk-based engines examine enhanced data streams that include device data, account profiles, and IP address, to which analytics and rules are applied to help the issuer selectively determine which transactions are high-risk enough to require stepped-up authentication. One-time passcodes (OTPs) and knowledge-based authentication (KBA) questions are increasingly used instead of the static password, and many of providers have biometric pilots underway as well. Table A provides a view into the use of various stepped-up authentication mechanisms by geography among issuers using RSA’s Adaptive Authentication for E-Commerce.

Table A: Stepped-Up Authentication Methods by Geography

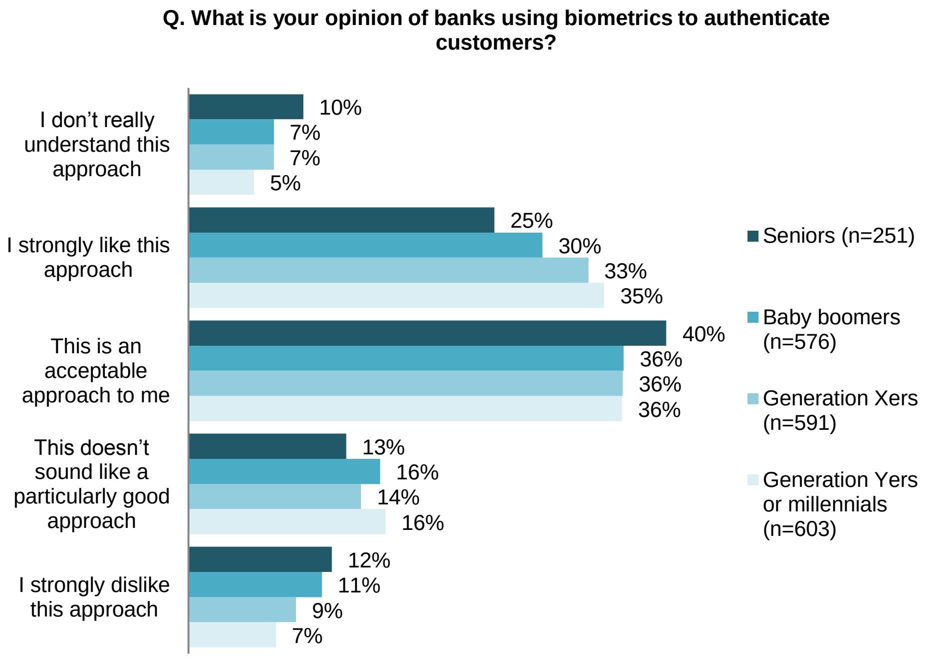
Geography	Data elements	OTP	KBA	Multiple challenge methods
Americas	100%	0%	7%	7%
Europe, the Middle East, and Africa	90%	28%	7%	31%
Worldwide	93%	18%	7%	23%

Source: RSA

The use of KBA is waning—many issuers are moving to alternative mechanisms due to the difficulty many consumers have in answering the questions. Biometrics are nascent but hold a lot of promise. While the biometric implementations are still in pilot, biometric authentication is rapidly entering mainstream consumer acceptance, thanks to innovations such as Apple’s Touch ID, which renders biometrics not only acceptable but also cool. A Q2 2015 Aite Group survey of

U.S. consumers showed widespread willingness to use biometrics as a stepped-up authentication mechanism among consumers of all ages (Figure 4).

Figure 4: Acceptance of Biometrics Among U.S. Consumers



Source: Aite Group Q2 2015 survey of 2,021 consumers

MANDATES

Not only has the user experience evolved over the 17 years since 3DS' initial launch but the regulatory environment has, too. In response to rising CNP fraud, a number of countries have mandated the use of either 3DS or some form of multifactor authentication for CNP transactions. Notable examples include India, Singapore, and South Africa. In addition, Europe's second Payment Services Directive (PSD2) includes a mandate for multifactor authentication for Internet payments, and Australia is moving toward a blanket national requirement for 3DS for CNP transactions, which will begin to be implemented in early 2017. Many e-commerce merchants have global operations, and as long as they are adding 3DS to their fraud prevention infrastructure for certain countries, they are also including the capability in their global strategy.

MOBILE

While the 3DS standard does not yet explicitly contemplate mobile, mobile transaction volume and fraud are both on the rise. In the United States in 2015, 36% of the Thanksgiving weekend holiday e-commerce purchases came in via a mobile device, and the smartphone hit a tipping point in early 2015, when it outpaced the desktop for the online retail category. These trends are substantiated by data from RSA, which is seeing not only mobile transactions increase across geographies but also the amount of fraudulent transactions originating from the mobile channel, as follows:

- **United States:** The percentage of mobile 3DS transactions is up 34%; the percentage of fraudulent mobile transactions grew from approximately 7.5% of all transactions in Q1 2014 to more than 10% in Q4 2015.
- **Australia and New Zealand:** The percentage of mobile 3DS transactions is up 28%; the percentage of fraudulent mobile transactions grew from approximately 7.5% of all transactions in Q1 2014 to just under 10% in Q4 2015.
- **Continental Europe:** The percentage of mobile 3DS transactions is up 24%; the percentage of fraudulent mobile transactions grew from approximately 4% in Q1 2014 to approximately 7.5% in Q4 2015.
- **U.K.:** The percentage of mobile 3DS transactions is up 20%; the percentage of fraudulent mobile transactions grew from 17% in Q1 2014 to just over 26% in Q4 2015.

3-D SECURE 2.0

While 3DS has come a long way since its initial release, industry stakeholders are actively working to update the 3DS specification. Work on the new specification is underway, with the goal of a mid-2016 release. The new and improved version will feature a number of enhancements:

- **More data elements:** The issuer will receive more data about the transaction from the merchant, including transactional data as well as contextual. This will enable improved detection rates and further reduce the number of transactions requiring stepped-up authentication.
- **Mobile-friendly 3DS:** As noted earlier, increasing numbers of transactions are originating from mobile devices, while 3DS still relies on HTTPS sessions. While there are workarounds, the 3DS spec will contemplate a mobile-app-friendly environment.
- **Improved consumer experience:** This will minimize the use of static passwords, codify the elimination of pop-up boxes, and reduce transaction latency.

CONCLUSION

The rising tide of CNP fraud means issuers and merchants alike need to deploy more robust fraud-prevention mechanisms to stem losses and preserve the customer experience. Here are a few recommendations:

Issuers:

- **If you can't support risk-based 3DS today, put that on your near-term roadmap.** Merchants are increasingly embracing 3DS; this combined with the rising tide of CNP fraud in general spells imminent pain in the form of increasing CNP losses and a degrading customer experience for issuers that delay.
- **Look to OTP, data elements, and biometrics for step-up.** KBA is falling from favor, due to the double whammy of customer friction and the relative ease with which fraudsters can game the system. OTP and data elements are leading the way in terms of issuer adoption and customer preference, and many see biometrics as the potential authenticator of choice in the future.
- **Educate, educate, educate.** Issuers need to set appropriate expectations about the potential changes to the customer experience, so when stepped-up authentication is required, the customer understands that the financial institution is trying to protect them, not inconvenience them.

Merchants:

- **Add 3DS to your fraud-prevention arsenal.** You don't have to send all your transactions across the 3DS rails unless you're in a geography that mandates this. 3DS can be a very effective tool, however, and with no end in sight to the continued pressure on CNP transactions, 3DS can be one more effective tool at your disposal.

ABOUT AITE GROUP

Aite Group is an independent research and advisory firm focused on business, technology, and regulatory issues and their impact on the financial services industry. With expertise in banking, payments, securities & investments, and insurance, Aite Group's analysts deliver comprehensive, actionable advice to key market participants in financial services. Headquartered in Boston with a presence in Chicago, New York, San Francisco, London, and Milan, Aite Group works with its clients as a partner, advisor, and catalyst, challenging their basic assumptions and ensuring they remain at the forefront of industry trends.

AUTHOR INFORMATION

Julie Conroy
+1.617.398.5045
jconroy@aitegroup.com

CONTACT

For more information on research and consulting services, please contact:

Aite Group Sales
+1.617.338.6050
sales@aitegroup.com

For all press and conference inquiries, please contact:

Aite Group PR
+1.617.398.5048
pr@aitegroup.com

For all other inquiries, please contact:

info@aitegroup.com

ABOUT RSA

RSA helps organizations reduce the risks of operating in a digital world. RSA solutions give customers the ability to detect, investigate, and respond to advanced threats; confirm and manage identities; and ultimately, reduce IP theft, fraud, and cybercrime. For more information on RSA, please visit www.rsa.com.

ABOUT RSA ADAPTIVE AUTHENTICATION FOR ECOMMERCE

RSA Adaptive Authentication for eCommerce is a risk-based authentication solution that evaluates more than 100 fraud indicators to determine the risk level of Web and mobile transactions in real time. Based on the 3-D Secure protocol, Adaptive Authentication for eCommerce enables merchants and issuers to offer additional cardholder protection and mitigate the risk of chargeback losses while maintaining a consistent, secure online shopping experience for cardholders. Supported by the RSA eFraudNetwork, Adaptive Authentication for eCommerce boasts consistently high fraud detection rates of approximately 95%, which is achieved with extremely low intervention and false positives.

CONTACT

For more information on RSA products and services, please contact:

RSA Sales
+1.800.495.1095