Aite PARTNER. ADVISOR. CATALYST.

Mobile Capture and Identity Verification: More Acquisitions, More Securely

Prepared for:

TABLE OF CONTENTS

LIST OF FIGURES

INTRODUCTION

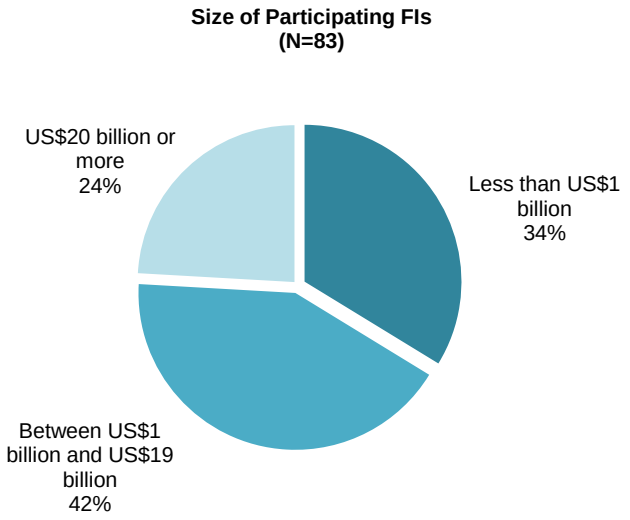
New-account acquisition is an increasingly challenging proposition for financial institutions (FIs). Consumers are transitioning their activity to the online and mobile channels, particularly the digital-native millennials. Dodd-Frank dramatically changed the economics of retail banking in the United States, and the Consumer Financial Protection Bureau is intensely scrutinizing new-account risk assessment practices. Fraud is on the rise, fueled by reams of personal data compromised in data breaches. If all that weren't enough, a number of technology companies are looking to nip away at various banking services in an effort to displace the traditional banking relationship.

As FIs work to stay relevant with consumers of all ages, the mobile channel has increasing importance. A strong mobile presence is increasingly table stakes for FIs looking to ward off the Huns clamoring at the gates. One key component of this is a mobile data capture and identity document verification capability, which can convert the mobile onboarding process from arduous to easy and make it more secure. This white paper examines the challenges facing FIs and discusses how mobile data capture and identity verification can help FIs with some of their key new-account acquisition goals.

METHODOLOGY

This white paper is informed by data from ongoing conversations with industry executives, desk research, and a Q4 2015 Aite Group survey of 88 executives from 83 U.S. FIs (Figure 1). The data from the total sample has a 10.5-point margin of error at the 95% level of confidence.

Figure 1: Size of Survey Participants

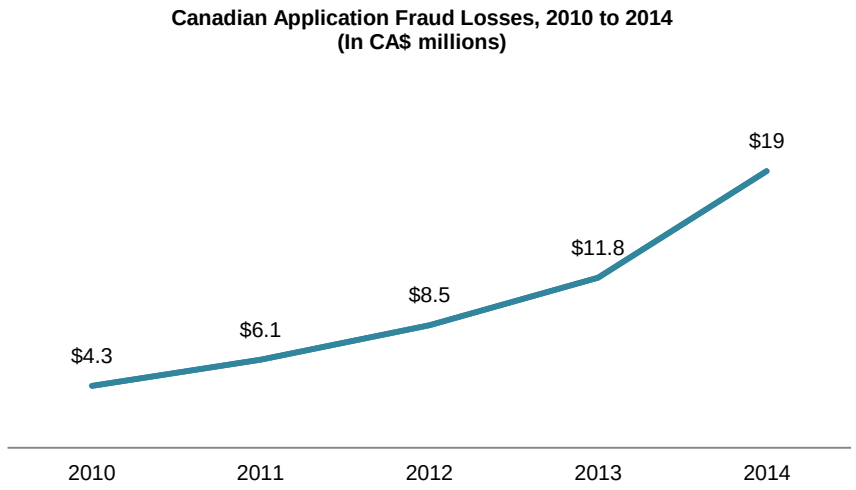


Source: Aite Group survey of 83 U.S. FIs, November to December 2015

THE RISING TIDE OF APPLICATION FRAUD

A benefit of being the last G-20 country to migrate to EMV is that there are plenty of lessons the U.S. can learn from the countries that preceded it. Canada's experience is a prime example of the fraud migration that takes place; while counterfeit card fraud sharply declines, FIs see a corresponding increase in other forms of fraud as fraudsters shift tactics to backfill the gap in their illicit revenue. Canada saw its application fraud losses increase nearly 500% in the wake of its EMV migration. Fraudsters could no longer buy stolen card numbers in the underweb and use them to fabricate counterfeit cards, so they switched instead to buying personal identifying information (PII) to get cards of their own using stolen and synthetic identities (Figure 2).

Figure 2: Canada's Increasing Application Fraud Losses



Source: Canadian Bankers Association

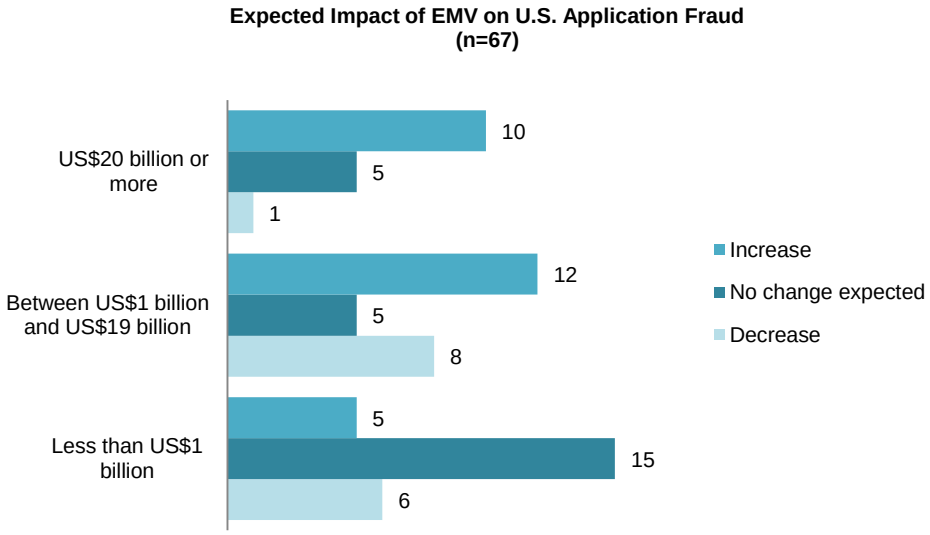
The blame for rising application fraud cannot be solely placed on the EMV migration. 2014 and 2015 also saw scores of major data breaches; 278 million records were breached in 2015 alone, many of which included PII.[1] These breaches have provided criminals with an ample inventory of PII, which they are now using to perpetrate identity fraud.

As a result of these converging forces, more than half of the large FI executives surveyed believe that application fraud in the United States will follow the example of its northern neighbor (Figure 3). Interestingly, the expectations differ widely among the largest institutions versus the midsize and the small. Part of this divergence in expectation could be because many large FIs are already seeing escalating losses. A number of executives at institutions with more than US$20 billion in assets state that the criminals did not wait for the October 1 liability shift date; their FIs saw steadily rising application fraud losses over the course of 2015. Another part of the

1. Breach Level Index, accessed on December 30, 2015, http://breachlevelindex.com.

divergence is likely attributable to the fact that credit cards represent an especially attractive target for cybercriminals, and large FIs own a disproportionate share of the credit card market.

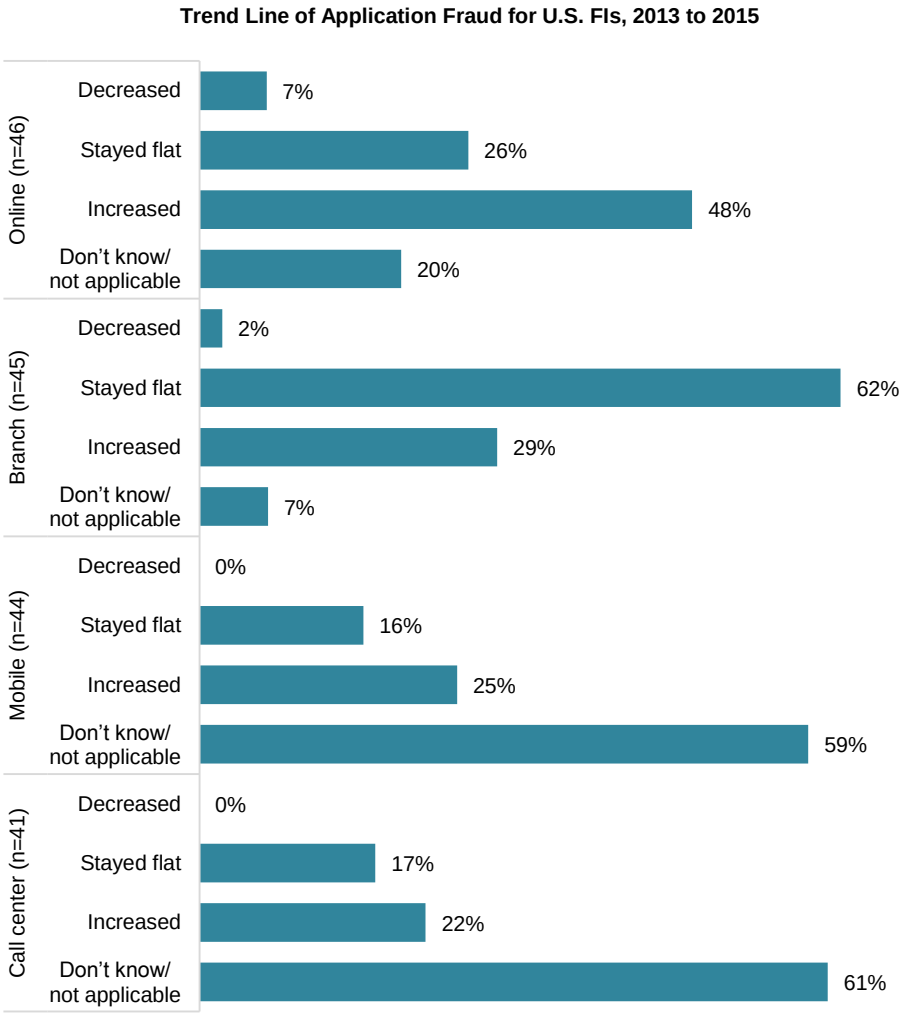
Figure 3: EMV's Anticipated Impact on U.S. Application Fraud



Source: Aite Group survey of 83 U.S. FIs, November to December 2015

The big FIs are not the only ones seeing rising application fraud losses. The majority of FIs surveyed say that application fraud has increased in the online, mobile, and call center channels over the past two years (Figure 4). The branch fraud rate has stayed flat for the majority of respondents, reflective of the fact that fraud is much easier to perpetrate in a faceless environment.

Figure 4: U.S. Application Fraud Trend Line



Source: Aite Group survey of 83 U.S. FIs, November to December 2015

MOBILE: THE SECURE ACQUISITION OPPORTUNITY

Mobile is increasingly the device of choice for consumers. Sixty-eight percent of the U.S. consumer population now owns a smartphone, and the 2015 holiday season substantiated the migration to mobile devices.[2] 2015 holiday e-commerce sales were up 20% over 2014 in the United States; 30% of those sales originated from the mobile channel, versus 25% in 2014.[3,4] U.S. mobile banking logins hit the tipping point in 2013, when mobile banking logins exceeded online banking logins for the first time. That doesn't mean there are more mobile bankers (yet), but rather that mobile bankers are more engaged, logging in 15 to 20 times per month, versus the three to five times that online bankers average.[5]

Maximizing the mobile channel isn't as easy as porting an online website over to a mobile device. The screen and keyboard are much smaller, which complicates the process of creating an elegant user experience. This challenge is compounded by the fact that innovation is rife in the mobile channel, and consumers' (particularly millennials') expectations for a user-friendly mobile commerce experience are shaped by brands such as Apple, Amazon, and Uber.

In spite of the momentum toward mobile, applications originating from the mobile channel have been lagging thus far. A Q1 2015 Aite Group survey of consumers showed that fewer than 3% of consumers actually complete an application for a checking account via a mobile device—many who start there give up and wind up in a branch (or at a competitor).[6] One of the inherent challenges to mobile account acquisition is smaller real estate, both in terms of screen size and keyboard.

Mobile data capture and verification solutions can be a very effective solution to this problem. These solutions use the camera on the mobile device to capture a picture of an identity credential (e.g., a driver's license), verify the credential, and parse the data into the onboarding system, eliminating the need for consumers to go through the data entry process.

Aite Group asked FIs about their plans with regard to implementing mobile data capture and verification solutions (Figure 5). The percentage of FIs with solutions either in place or in the implementation process are fairly equally split among large, midsize, and small FIs, at 13%, 20%,

2. Monica Anderson, "The Demographics of Device Ownership," Pew Research Center, October 29, 2015, http://www.pewinternet.org/2015/10/29/the-demographics-of-device-ownership/.

3. Sarah Halzack, "Retailers Ring Up Healthy Sales This Holiday Season," The Washington Post, December 28, 2015, https://www.washingtonpost.com/news/business/wp/2015/12/28/retailers-ring-up-healthy-sales-this-holiday-season/.

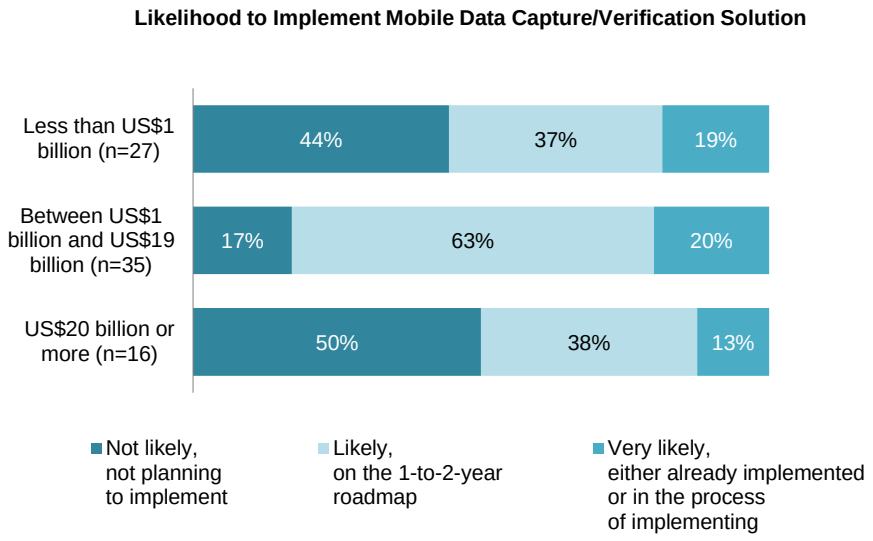
4. Tracy Maple, "Mobile Devices Deliver Holiday E-commerce Sales," Internet Retailer, January 6, 2016, https://www.internetretailer.com/2016/01/06/mobile-devices-deliver-holiday-e-commerce-sales.

5. See Aite Group's report *U.S. Online Banking Vendors and Their Consumer Online Banking Solutions*, July 2014.

6. See Aite Group's report *U.S. Trends in Checking Account Opening*, October 2015.

and 19%, respectively. Thirty-seven percent of large FIs, 63% of midsize FIs, and 38% of small FIs have mobile data capture on their one-to-two-year roadmap.

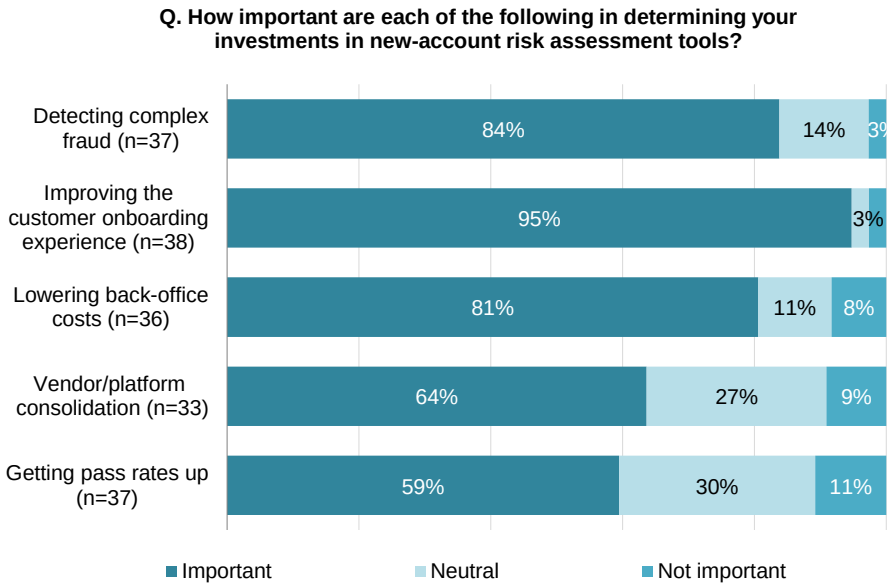
Figure 5: Propensity to Implement a Mobile Data Capture/Verification Solution



Source: Aite Group survey of 83 U.S. FIs, November to December 2015

Mobile data capture and verification can automate the data capture, vastly improving the customer experience and enabling mobile as a bona fide acquisition channel. It can verify the credential and automate the verification of the data, helping with fraud reduction. Finally, mobile data verification can automate the process of collecting and validating additional documents during the manual review process, lowering back-office costs. All of these points were highlighted as key drivers of FIs' new-account risk assessment investments by survey respondents (Figure 6).

Figure 6: Priorities Driving New-Account Risk Assessment



Source: Aite Group survey of 83 U.S. FIs, November to December 2015

For FIs that either have implemented mobile data capture or are in the process of doing so, customer experience and operational efficiency were highlighted in interviews as dual and equal drivers. Many FIs have ambitious goals for increasing originations via the mobile channel, and this will only be possible by making the process more user friendly. Reducing operational expense is another key goal. One large FI that is in the process of implementing a mobile data verification solution currently has 350 full-time employees dedicated to reviewing the exceptions from its application fraud review process. A big portion of this workload entails reviewing copies of driver's licenses, utility bills, etc., which consumers send in to validate their identities. This FI estimates that automating this via mobile data capture will enable it to cut that workforce in half.

CONCLUSION

FIs are facing a dual challenge of rapidly rising fraud and fierce competition in acquiring new customers. Here are a few recommendations for FI executives responsible for new-account acquisitions:

- **Prepare for an increase in application fraud.** As the U.S. migration to EMV progresses, fraudsters will increasingly look for new ways to perpetrate fraud. Based on the early experience of large FIs as well as data from countries whose EMV upgrades preceded that of the United States, application fraud will increase significantly.
- **Build your fraud-mitigation strategy with the assumption that the data has been compromised.** The days when personal data was actually private and confidential are long gone, thanks to the rampant trend of data breaches. This means FIs must use new means of verifying the data presented during the application process.
- **Create a delightful customer experience for your new applicants.** FIs are no longer just competing with each other, they're also competing with technology firms that have made digital transactions as easy and intuitive as possible for consumers. The consumer-expectation bar for mobile banking has risen substantially as a result.
- **Add mobile data capture and verification to your near-term roadmap.** Mobile data capture and verification can help with the challenge of risk assessment while at the same time improving the customer experience. Consumers are saved the need to type lots of data into a tiny little keyboard, and FIs can automate much of the back-end verification process.

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 MITEK

Mitek (NASDAQ: MITK) is a global leader in mobile capture and identity verification software solutions. Mitek's ID document verification allows an enterprise to verify a user's identity during a mobile transaction, enabling financial institutions, payments companies, and other businesses operating in highly regulated markets to transact business safely while increasing revenue from the mobile channel. Mitek also reduces the friction in the mobile user experience with advanced data prefill. These innovative mobile solutions are embedded into the apps of more than 4,500 organizations and used by tens of millions of consumers daily for new-account opening, insurance quoting, mobile check deposit, and more.

ABOUT MOBILE VERIFY

Mobile Verify, Mitek's ID document verification solution, assures that the ID presented in a mobile transaction is a genuine, unaltered, and government-issued ID. It provides consumers a fast and easy way to create a trusted identity with an organization anytime, anywhere. Mobile Verify enables businesses to safely and securely acquire new customers and complete high-value transactions in the mobile channel.

CONTACT

For more information on Mitek's mobile offering, please contact:

Mitek Sales
+1.858.309.1704
sales@miteksystems.com
www.miteksystems.com