Aite PARTNER. ADVISOR. CATALYST.

The Mobile Device: The Center of the Fraud Prevention Universe

JANUARY 2017

Prepared for:

TABLE OF CONTENTS

LIST OF FIGURES

INTRODUCTION

The bad guys are winning. This is the sentiment of many financial institution (FI) and merchant fraud mitigation executives, who are finding it increasingly difficult to keep pace with the rapidly changing fraud landscape. With nearly six billion data records compromised since 2013, the organized crime rings behind the majority of financial fraud have a treasure trove of data at their disposal. Personally identifiable information (PII) and login credentials are no longer reliable means of identifying customers, since FIs and merchants alike have to assume that the criminals already have this data in their possession.

At the same time that the threat environment is escalating, fraud executives face strong internal pressure to ensure that their risk controls do not adversely impact the customer experience. The new bar for customer experience has been set by Amazon 1-Click and Apple and, along with it, the customer expectation for elegant interactions with minimal friction.

Fortunately, a vision is emerging that balances effective fraud prevention with a delightful customer experience. Customer identification and authentication are no longer just about the customer's PII and static authenticators—in this environment, it is equally important to have a good understanding of the end user's digital identity and incorporate dynamic means of authentication. The mobile device sits at the center of this vision. Properly secured, the mobile device can not only facilitate safer transactions within its own channel but can also be used to better secure other channels with minimal customer friction. This white paper will delve deeper into this vision and the roadmap for forward-thinking fraud executives.

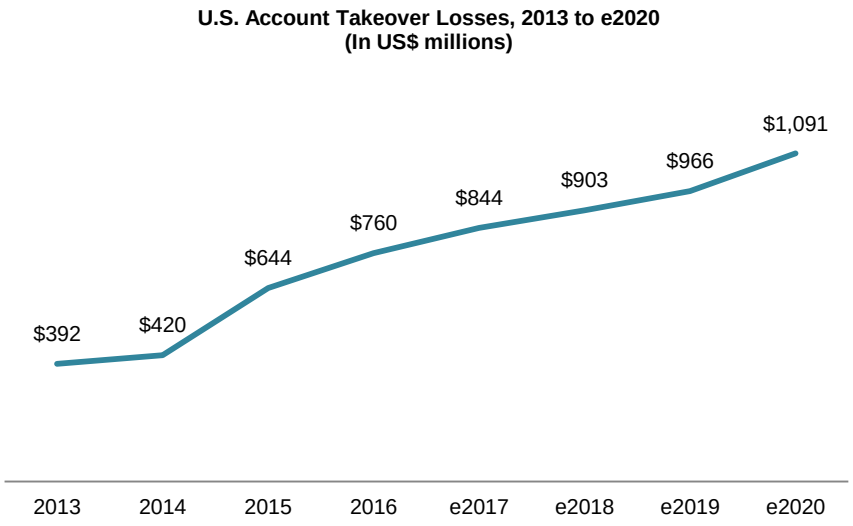
METHODOLOGY

This white paper is informed by Aite Group's ongoing discussions with fraud executives at large FIs, merchants, and payment networks in North America and Europe as well as a qualitative research study of 20 large North American issuers and processors in Q2 2016.

THE ESCALATING THREAT ENVIRONMENT

Due to the vast quantity of data in criminals' possession, FIs and merchants are seeing sharply rising levels of account takeover (Figure 1).

Figure 1: Rising U.S. Account Takeover Losses



Source: Aite Group

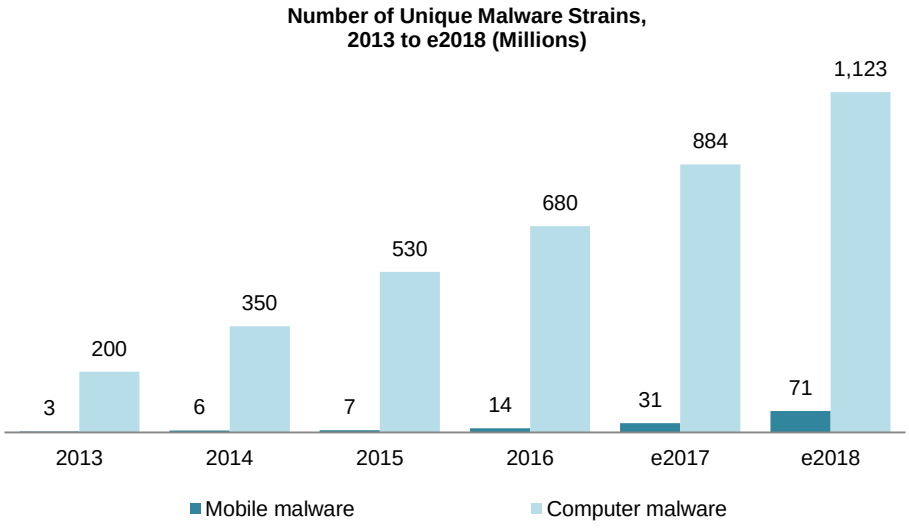
Criminal rings are using a wide variety of methods to breach FIs' and merchants' defenses and take over accounts. Key tactics include the following:

- **Social engineering:** Manipulating people to get them to surrender valuable information continues to be a key attack vector in fraud schemes; some of the favored current approaches include business email compromise and targeting contact centers. The contact center is particularly problematic for FIs right now—criminals will call into the contact center impersonating the customer, then gather data and/or change account settings that enable them to break into the customer's online account and drain it of funds.
- **Phishing:** Good old-fashioned phishing is still a remarkably effective weapon in criminals' arsenal. Phishing takes place when criminals send an email purporting to be from a trusted brand in an effort to gather personal information and/or credentials from the victim. This can either be by inducing the victim to click through to what he or she believes is the company's website and then input data, or by delivering a malware payload when the user clicks on a link or opens an attachment. Though customers are more aware of the issue than they were 10 years ago, criminals' attempts have also become much more sophisticated. In addition to polished-looking phishing attacks on the bank's own brand (now free of the spelling errors that characterized early phishing emails), the flurry of database breaches in

recent years also provides ample fodder for spearphishing attacks. (Spearphishing leverages the emails stolen in breaches, enabling the fraudster to tailor a more compelling email, given knowledge of an existing relationship between the victim and the breached entity.) Email-based phishing has also expanded to SMS-based phishing (smishing) and even voice calls (vishing).

- **Bots:** Bots are software applications that run automated scripts. While there are plenty of bona fide uses of this technology, criminals make ample use of it as well—bot attacks include everything from spam to denial of service to account takeover. A common use of bots for account takeover is to load compromised credentials into a series of bots (known as a botnet) and try them out on a multitude of banking and e-commerce sites, capitalizing on the fact that the majority of consumers still use the same set of login credentials across some or all of their online relationships. Bots can also be used for password cracking, in which repeated, automated attempts are made to guess the user's online password.
- **Malware:** The makers of malware continue to rapidly evolve their arsenal, as shown in Figure 2. Mobile malware continues to be dwarfed by the malware targeting computers, but it is growing at a rapid pace. Many FIs continue to report malware as a key loss driver, although it has decreased in severity from a few years ago.

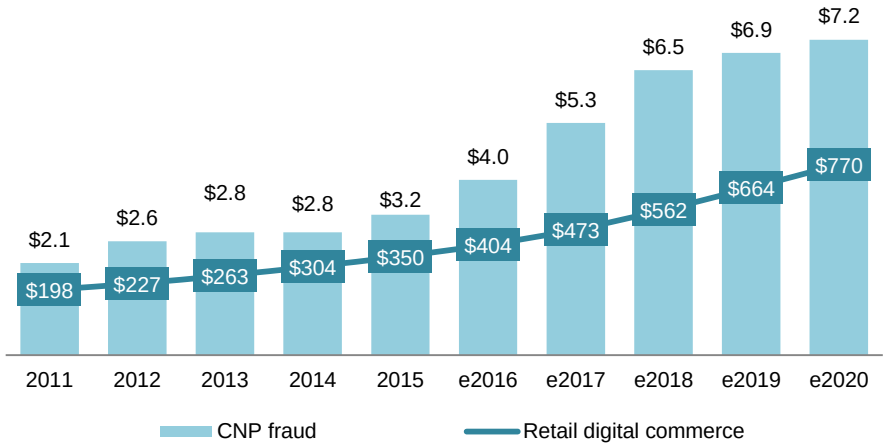
Figure 2: Malware Strains



Source: McAfee, Aite Group

Account takeover is not the only form of fraud on the rise. Card-not-present (CNP) fraud and application fraud are also rapidly rising, also fueled by the compromised personal data (Figure 3).

Figure 3: U.S. CNP Fraud Growth



Source: Aite Group

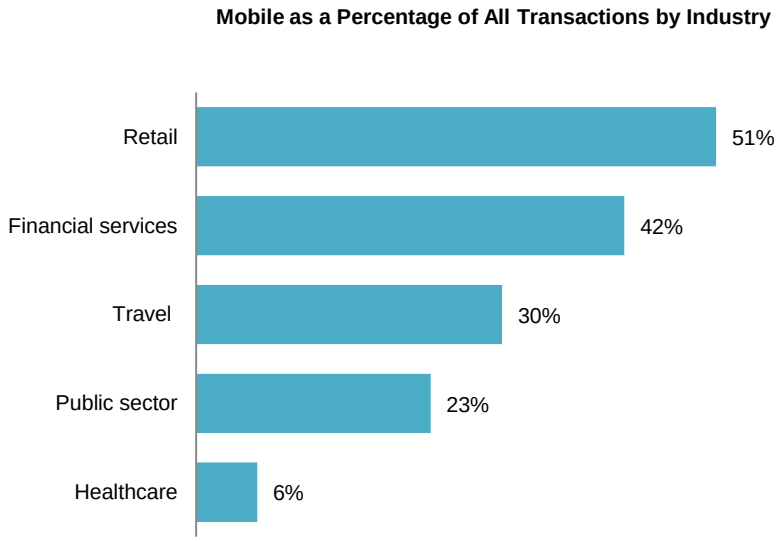
With the increasing use of 3-D Secure by merchants, CNP fraud is very much a shared problem for merchants and issuers. Unfortunately, the pace of increase for account takeover, CNP fraud, and application fraud will intensify as the U.S. migration to EMV proceeds and criminals are motivated to shift their tactics away from counterfeit fraud.[1]

1. See Aite Group's report: *EMV: Issuance Trajectory and Impact on Account Takeover and CNP*, May 2016.

MOBILE TO THE RESCUE

Against this daunting backdrop, fraud executives are finding that the increasing ubiquity of the mobile device presents new opportunities in fraud mitigation. Seventy-two percent of U.S. consumers, 68% of U.K. consumers, and 67% of Canadians now own a smartphone.[2] They are using these devices more and more for day-to-day activities. Fifty-one percent of transactions in retail e-commerce originate from the mobile device, and 42% of financial services' digital transactions are mobile (Figure 4).

Figure 4: Consumers' Mobile Device Usage by Industry



Source: iovation

The high levels of smartphone penetration and use represent a great opportunity to bring more security to transactions with minimal impact to the customer experience. The ubiquity and computing power of the smartphone enables it to serve as a form of security token—one that consumers willingly carry wherever they go and are likely to have in close proximity at all times. Properly secured, the mobile device can not only facilitate safer transactions within its own channel but can also be used to better secure other channels. The building blocks of this vision include the following technologies:

- **Geolocation**: Geolocation technology uses GPS to identify the position of the mobile device. Geolocation can be used in a number of ways—everything from geofencing (in which the customer identifies a range of trusted locations, such as "home" or "office" in which less authentication is required) to using proximity of the mobile

2. "Smartphone Ownership and Usage Continues to Climb in Emerging Economies," Pew Research Center, accessed on December 27, 2016, http://www.pewglobal.org/2016/.../smartphone-ownership-and-internet-usage-continues-to-climb-in-emerging-economies/.

device to a payment transaction as an additional factor in authorization risk assessment.

- **Device authentication:** Device authentication uses mobile carrier data to perform the same device hardware-based network authentication (e.g., SIM card) as mobile operators to secure a company's services and provide positive verification that the device belongs to the person authorized on the mobile account, to indicate whether the phone is prepaid or post-paid as well as to provide notification if the device is lost or stolen.
- **Device identification and risk assessment:** Once the device is authenticated, the business must continually verify and assess risk of the device itself. Device fingerprinting technology is particularly effective on the mobile device, since it offers such a wealth of data that can be ingested and analyzed (Figure 5). This results in a long-lasting and highly reliable device identification capability.
- **Risk-based authentication:** Based on the risk analysis performed in all of the preceding steps, businesses may choose to perform some form of authentication, commensurate with the risk of the transaction. This can be accomplished using a one-time password that is pushed from the mobile application, a fingerprint biometric, or facial recognition, among other forms of stepped-up authentication.

Figure 5: Mobile Device Identification

Source: iovation

Large banks are the leaders in executing against this vision; a few have already embedded many elements of this into their mobile app. With enough knowledge about the mobile device and its users, businesses can enable higher-risk transactions or actually begin performing stepped-down authentication (i.e., reducing the amount of friction for customers). The following provide some real-world applications of this concept:

- **Contact center:** When a consumer calls into the contact center using his or her secured and identified mobile device, the business can skip the usual round of challenge questions and just address the customer's need.
- **Payment card authorization:** Payment card authorization can be enhanced in a couple of ways using the mobile device. FIs can use mobile geolocation to determine whether the mobile device is in close proximity to a payment card transaction and reduce false positive declines. Some FIs are also using two-way text or mobile app push to engage the customer and verify anomalous payment card transactions.
- **Online verification:** The mobile device can be used to better secure online experiences in a variety of ways. Using geolocation, the proximity of the mobile device to the online session can be used as a factor of authentication and will remove the need for stepped-up authentication for lower-risk transactions. For higher-risk transactions, such as funds transfers, various forms of stepped-up authentication can be invoked via the mobile device, such as a one-time password pushed from the mobile app or a biometric. The latter authentication scenario is particularly secure, since it is validating not only something users have but also something they are.

Customer education is important, too. While less necessary in the contact center scenario, when nothing new is being asked of the customer, FIs need to be prepared to provide clear messaging to the customer when biometrics or other forms of stepped-up authentication are invoked so that customers know what they need to do, how, and why.

The smartphone is a powerful tool in the arsenal of fraud executives as they strive to strike that difficult balance between fraud mitigation and the user experience. Over the coming months and years, expect to see this device play an increasingly pivotal role in financial institutions' fraud mitigation strategies.

CONCLUSION

Criminals' nimbleness and innovation dictate that FIs and merchants need to be equally adept in their defensive tactics in order to preserve both the bottom line and the customer experience. Here are a few recommendations:

- **Harness the power of the mobile device.** Robust security on the mobile device has the potential to not only better secure mobile channel transactions but also add security and enhance the user experience in all other channels.
- **Convert data to intelligence.** Banks have a wealth of data at their disposal. Those that are harnessing that data to convert it into actionable intelligence are reaping the benefits in the form of better fraud prevention and less friction for customers.
- **Plan for continued investment in remote channel security.** Businesses that don't actively invest in their online and mobile security will get left behind by their competitors.
- **Educate your customers.** Clear education is a must anytime a new form of authentication that requires customer participation is inserted into the user experience. FIs need to clearly explain to customers *what* they need to do, *how* they need to do it, and the reason *why* they need to do it.

ABOUT AITE GROUP

Aite Group is a global research and advisory firm delivering comprehensive, actionable advice on business, technology, and regulatory issues and their impact on the financial services industry. With expertise in banking, payments, insurance, wealth management, and the capital markets, we guide financial institutions, technology providers, and consulting firms worldwide. We partner with our clients, revealing their blind spots and delivering insights to make their businesses smarter and stronger. Visit us on the web and connect with us on Twitter and LinkedIn.

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 IOVATION

iovation protects online businesses and their end users against fraud and abuse, and identifies trustworthy customers through a combination of advanced device identification, device reputation, multifactor authentication and real-time risk evaluation. More than 3,500 fraud managers representing global retail, financial services, insurance, social network, gaming and other companies leverage iovation's database of billions of Internet devices and the relationships between them to determine the level of risk associated with online transactions. The company's device reputation database is used to protect 18 million transactions and stop an average of 300,000 fraudulent activities every day. The world's foremost fraud experts share intelligence, cybercrime tips and online fraud prevention techniques in iovation's Fraud Force Community, an exclusive virtual crime-fighting network.

CONTACT

For more information on iovation's products and services, please contact: info@iovation.com or 1.503.224.6010.