PARTNER. ADVISOR. CATALYST.

Citadel and Gozi and ZeuS, Oh My!

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

INTRODUCTION

ZeuS, OddJob, Gozi Prinimalka, Citadel—the ever-growing variety of malware actively targeting banks and their customers is having a marked impact on the financial services industry. The malware, which consists of sophisticated, ever-evolving pieces of software designed to compromise online banking credentials, is deployed by international organized criminal rings that are nimble, innovative, and constantly evolving their attacks on financial institutions (FIs) and their customers.[1]

Cyberthreats are growing at a frightening pace, with more than 100 million unique strains of malware detected in Q2 2012 representing a 25% increase in the malware population in just nine months. More than 100,000 unique new strains of malware targeted at the online channel are being deployed *every day.* Mobile malware is also on the rise, with unique strains doubling between Q2 2012 and the same quarter the previous year.[2] A significant portion of the malware is specifically designed to log the keystrokes of customers as they are entering their online banking credentials. Once the credentials are compromised, the cybercriminals then use them to log into online banking accounts and drain them of funds.

In the face of this threat environment, FIs and their customers need to be more vigilant than ever and continue to deploy their own innovative techniques to protect their financial information. Session-based security is no longer enough. Regulators advocate multiple layers of security, a strategy that is already in use at many financial institutions. This approach combines a number of different, complementary technologies that protect against the wide variety of attack vectors. Because the bad guys have proven adept at compromising in-progress Web sessions, security must take a holistic approach, securing not only the session but also the transaction itself.

This white paper will provide an overview of the latest techniques and tactics that cybercriminals are successfully using to perpetrate their corporate account takeover attacks, quantify the impact of those strategies on financial institutions, and recommend ways in which banks can protect themselves and their customers.

MAN-IN-THE-BROWSER ATTACKS

Man-in-the-browser (MitB) attacks, deployed in the form of the ZeuS Trojan and its numerous offspring, have rapidly turned into the bane of FI fraud executives' existence. A pernicious form of malware, keylogging Trojans record end users' online banking credentials and send them to cybercriminals, who then use them to log into the online banking site and drain the account.

[1] For a primer on cybercrime threats, see Aite Group's report, *Banks and Businesses in the Crosshairs: Cybercrime and Its Impact*, September 2011.

[2] McAfee Threat Report: Third Quarter 2012, http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q3-2012.pdf

Trojans are prolific, thanks to their ability to be run in an automated fashion. RSA estimates that 80% of corporate account takeover attacks involve the use of the ZeuS Trojan.[3]

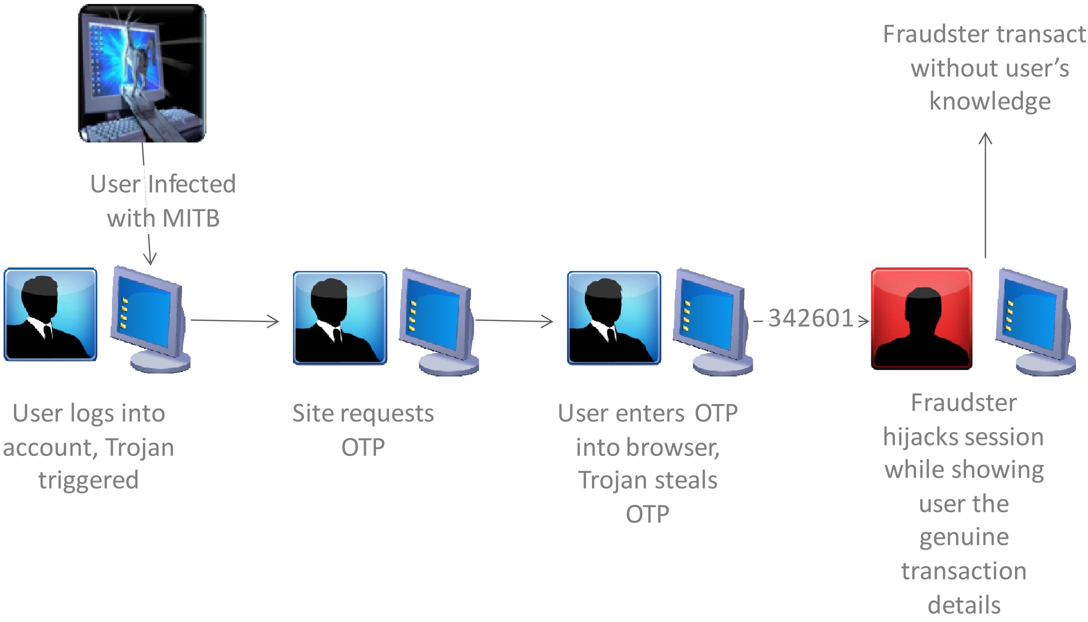
While FIs have responded in the form of additional layers of defense, malware inventors are nothing if not creative. They have shown a talent for rapidly evolving their software to contravene many online fraud-mitigation technologies. A prime example of this is a variant of the OddJob Trojan that is bypassing multiple controls and causing significant losses. Here's how it works:

- **Step 1:** Once downloaded to the victim's computer, OddJob captures all online credentials (including one-time passwords).
- **Step 2:** The malware then posts a fake Web page designed to make the end user believe that his or her session has been either stalled or terminated.
- **Step 3:** Leveraging the active session, the cybercriminal will use the compromised credentials to initiate an Automated Clearing House (ACH) or wire transaction.
- **Step 4:** The malware will then inject a fake Web page, so the next time the victim logs in, he or she sees the expected account balance. It typically takes a few days for the theft to be discovered, by which time it's impossible for the bank to recoup the funds (Figure 1).

This attack vector is particularly ingenious because it bypasses multiple fraud-mitigation controls at once. Device fingerprinting is rendered useless because the cybercriminal is using an active session that looks like it is originating from a trusted device. One-time password tokens are of no use because the malware steals the password and invokes it at the time of transaction. As part of ongoing research into the online and mobile threat environment, Aite Group interviewed fraud executives from 15 of the top 35 North American FIs between August and November 2012. One bank stated that after successfully preventing all corporate account takeover losses during the prior two years, this particular attack vector resulted in three corporate account takeover losses in 2012, totaling nearly US$1 million.

[3] RSA 2012 Cybercrime Trends Report, http://www.rsa.com/products/consumer/whitepapers/11634_CYBRC12_WP_0112.pdf

Figure 1: Trojans Bypass Two-Factor Authentication


User Infected with MITB
User logs into account, Trojan triggered
Site requests OTP
User enters OTP into browser, Trojan steals OTP
342601
Fraudster hijacks session while showing user the genuine transaction details
Fraudster transacts without user's knowledge

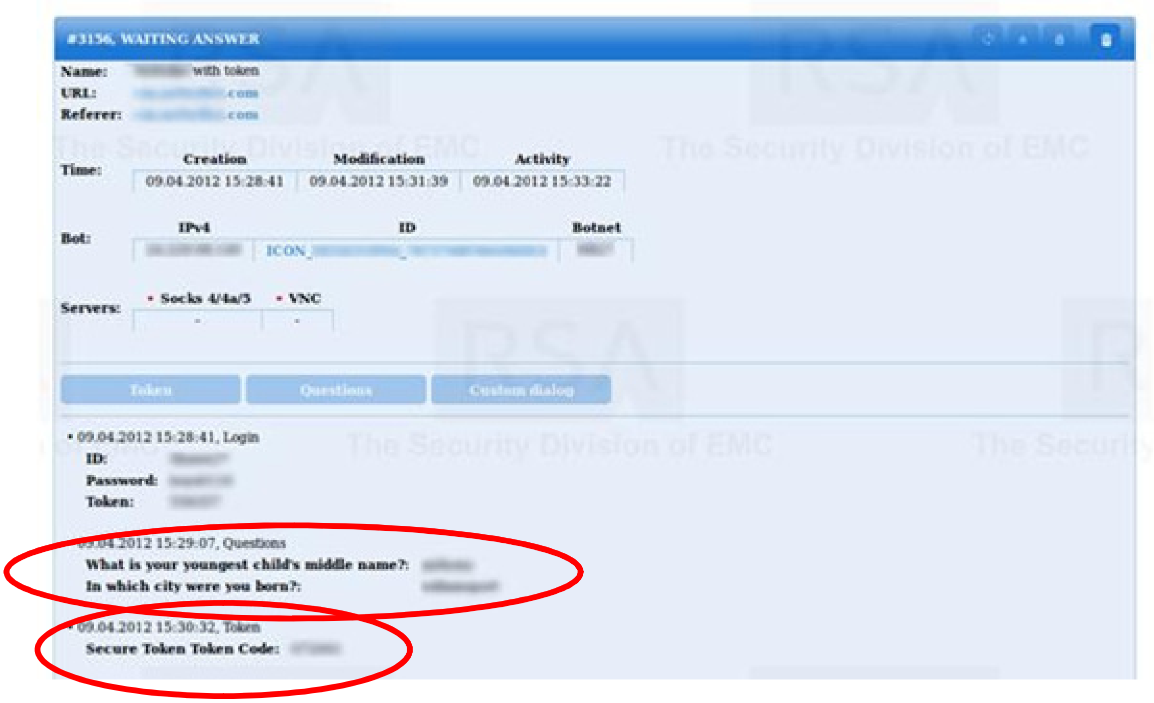
Source: RSA

MAN-IN-THE-MIDDLE ATTACKS: INCREASING USE OF MANUAL ATTACKS

Another way in which cybercriminals are adapting is by returning to manually driven attacks in response to the increasing use of behavioral analytics that can detect the navigation patterns indicative of an automated attack. In a manually controlled attack, the perpetrator sits in the middle in order to be able to respond in a dynamic fashion to the FI's security protocols (thus the sobriquet "Man-in-the-Middle" or MitM). While by no means new in concept, the current MitM methodologies have significantly evolved in their sophistication.

Figure 2 provides a screenshot that exemplifies how this attack works. An attacker inserts him or herself in the communication stream between the end user and the bank and performs HTML injection on the fly, often using a set of templates prepared in advance. This enables the attacker to collect all of the data necessary to bypass security controls and initiate transactions. As can be seen from this example, the attacker was able to successfully collect the credentials at login, then prompted the end user to input the answers to static challenge questions: "What is your youngest child's middle name?" and "In what city were you born?" The attacker also successfully collected the PIN for the one-time password token. Armed with this data, the attacker then has the ability to navigate through the banking session and initiate illicit transactions.

Figure 2: Screenshot from Man-in-the-Middle Attack



#3156, WAITING ANSWER

Name: [redacted] with token
URL: [redacted].com
Referer: [redacted].com

Time:

Creation	Modification	Activity
09.04.2012 15:28:41	09.04.2012 15:31:39	09.04.2012 15:33:22

Bot:

IPv4	ID	Botnet
[redacted]	ICON_[redacted]	[redacted]

Servers:

• Socks 4/4a/5	• VNC
-	-

• 09.04.2012 15:28:41, Login
ID: [redacted]
Password: [redacted]
Token: [redacted]

• 09.04.2012 15:29:07, Questions
What is your youngest child's middle name?: [redacted]
In which city were you born?: [redacted]

• 09.04.2012 15:30:32, Token
Secure Token Token Code: [redacted]

Source: RSA

MOBILE IS NOT EXEMPT

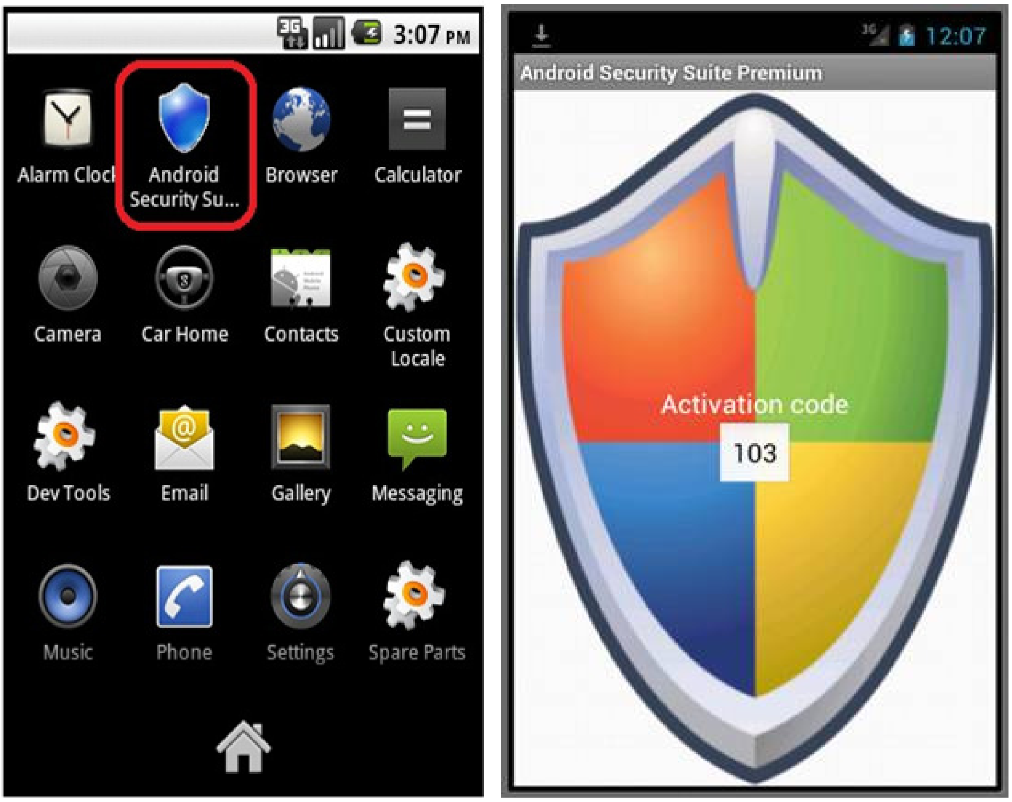
While the number of malware threats in the mobile environment is still far fewer than online, this platform is by no means exempt. Notably, attackers are already deploying malware designed to perpetrate cross-channel attacks. A prime example of this is Citadel-in-the-Mobile attacks (CitMo), designed to intercept SMS-based one-time passwords. While SMS hijacking is not new in and of itself, the sophistication that is evident in CitMo is causing pain for FIs. (There are also closely related variants such as ZeuS-in-the-Mobile attacks).

Here’s how it works: The targets of these attacks are typically small businesses or high-net-worth individuals that use an SMS one-time password to authorize transactions on their online banking site. The user has already unwittingly downloaded a Trojan onto his or her computer, which facilitates Step 1 of the following process.

- **Step 1:** The user logs into the online banking site and is presented with a message that says that the mobile security is insufficient and the user needs to download the “Android Security Suite.”
- **Step 2:** The message prompts for an activation code that they will receive upon downloading the application to the mobile phone.
- **Step 3:** Once the user downloads the “app” on his or her phone, the app provides the activation code, which the user enters where prompted on the PC screen.

- **Step 4:** The submission of the activation code alerts the attacker that the mobile malware has successfully been installed and that it is now safe to proceed with the online theft.
- **Step 5:** The attacker proceeds with a standard Trojan-based attack. When the bank sends the user the SMS one-time password, the malware on the mobile device re-routes that SMS to the attacker, who uses it to complete the transaction (Figure 3).

Figure 3: Screenshots From a CitMo Attack

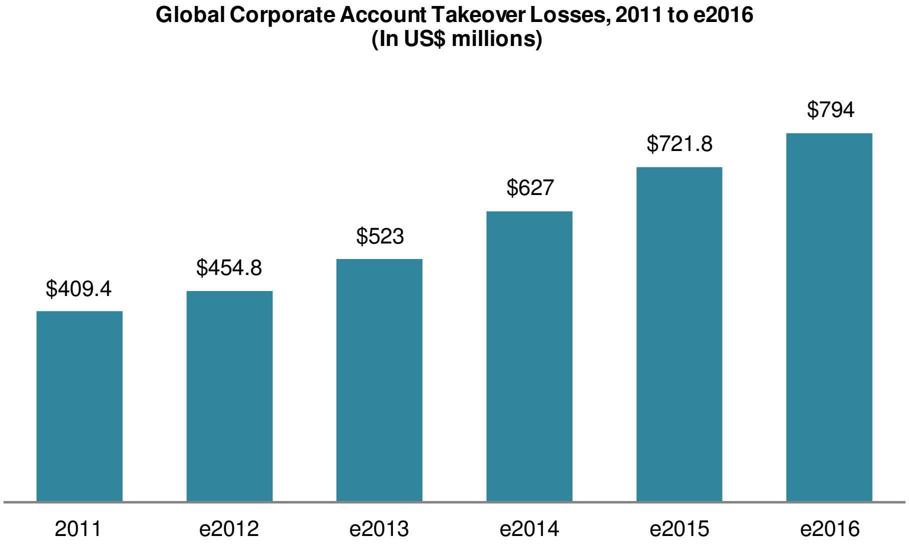


Source: Kaspersky Labs, RSA

THE GLOBAL IMPACT OF ACCOUNT TAKEOVER

The impact of these attacks is significant. Losses from corporate account takeover will cost banks and business around the world US$454.8 million in 2012, and it will grow to US$794 million in 2016 (Figure 4). North America and Europe are feeling the brunt of the impact today, but the growth rate of the fraud is increasing more rapidly in the Asia-Pacific and South America.

Figure 4: The Global Impact of Corporate Account Takeover



Source: Aite Group

IN SEARCH OF STRONGER DEFENSES

In response to the morphing threat environment, banks continue to evolve their security. Given the ease with which malware can bypass session-level security, many FIs are focusing on ways in which they can protect the transaction itself. Transaction-level security can be achieved in a number of ways, as shown in Table A.

Table A: Transaction-Level Security Options

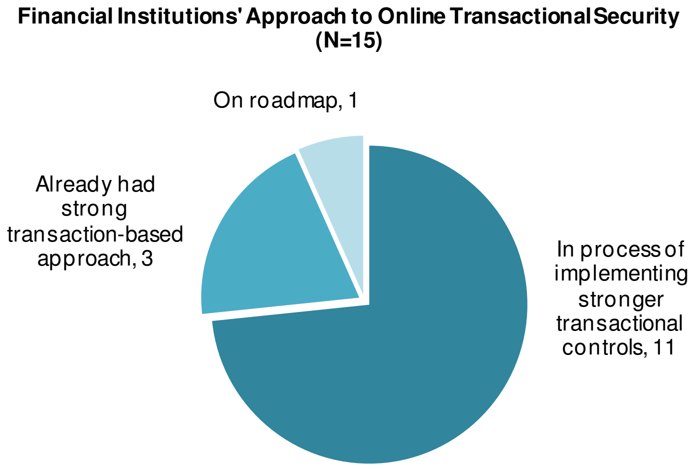
Technology	Description	Aite Group's take
Device fingerprinting	Device fingerprinting is the ability to look at a combination of identifiable hardware and software attributes associated with a computer or mobile device. The unique fingerprint associated with each device can be used to provide recognition of devices associated with fraudulent activity as well as ongoing recognition of devices with trusted reputations. This differs from simple device printing that only leverages cookies, which the recent Federal Financial Institutions Examination Council (FFIEC) guidance deemed inadequate. It is also important for a device fingerprinting solution to be able to detect the use of proxies. Cybercriminals use proxy servers to log on to banks from a proxy IP address that allows penetration of user accounts via the genuine end-user IP to gain positive device identification. Proxy attack detection can determine when a login or transaction is being performed via a proxy that is anomalous to the user by identifying the true IP used.	Device fingerprinting is a great front-line technology that can help eliminate a wide swath of the fraudsters that target FIs on a daily basis. It is susceptible to MitB attacks, however, and needs to be deployed in conjunction with other technology that can focus on the transaction itself.
Behavioral analytics	Through rules and/or analytics, behavioral analysis tools detect fraud by monitoring the user session to detect suspicious activities or patterns. Behavior analysis technologies can also examine Web navigation techniques to highlight anomalies indicative of suspicious activity.	Behavioral analytics represent a great way to detect pattern anomalies and are a key technology that FIs are looking to as they seek to bring their fraud-mitigation technologies down to the transaction level. As with any tool, there is a certain level of false positives, and it is good to have a stepped-up authentication capability available to include the end user in the triage process.
Trojan detection	Once resident on a user's computer, there are a couple of key ways in which technology can be used to detect indicators of Trojan activity: **HTML injection detection:** Detects and flags fraudulent changes to end users' browser display via MiTB attacks, which attempt to	Increasingly, the end user's endpoint is compromised, so it is incumbent upon FIs to have technology in place that can detect the compromise and alert the bank. Fortunately, there are telltale signs common to most Trojans that sophisticated

Technology	Description	Aite Group's take
	either manipulate payments or harvest additional user credentials like a Social Security number, credit card number, or PIN. **Man vs. Machine protection:** Defends against advanced Trojans using automated script attacks to fraudulently add payees and transfer money to mule accounts. Man vs. Machine protection can determine whether mouse or keystroke movements are associated with user-directed actions.	technology is able to detect and flag.
Knowledge-based authentication (KBA)	KBA questions seek to establish the authenticity of the end user by asking questions only that individual should know. KBA questions are either static (preset at the time of account setup) or dynamic (multiple-choice questions are gleaned from databases including credit and/or demographic data).	Static KBA questions are largely ineffective, thanks to the ready availability of personal data on the Internet. Dynamic KBA is more effective, but the cost is often high enough that FIs are judicious in its use.
One-time password tokens	A one-time password token supplies an expiring password, which changes on either an event- or time-driven basis. The token can either be a physical token or a software-based token that resides on a PC or mobile device.	One-time password tokens are a tried and true method of fraud mitigation and still highly effective, particularly when deployed in conjunction with dual control requirements. As described in the OddJob example, however, the success of the solution has created an incentive for the makers of malware to successfully devise a workaround.
Out-of-band authentication (OOBA)	OOBA uses a communication mechanism that is not directly associated with the device being used to access the banking application in order to facilitate a second mode of communication. This is often accomplished by using a mobile device in conjunction with an online session to deliver a one-time password.	This technology is increasingly being deployed by FIs to commercial and retail customers alike. It has many of the security benefits of an OTP token, without the overhead of having to deploy and maintain the hardware. While susceptible to CitMo, ZitMo, et al, the added requirement of socially engineering the end user and deploying malware to two separate devices is a significant hurdle for the would-be attacker to overcome.
Transaction signing	Transaction signing requires the end user to digitally sign each transaction. The approach can vary: some signing solutions use public key infrastructure on a hardware device, other solutions enable the end user's mobile device with the signing solution.	Transaction signing offers the benefits of OOBA, without the downside risk of the SMS being hijacked, since the signing key is calculated and pushed from an app native to the device. It also is a good solution to MitM, as it gives the end user the opportunity to view the transaction parameters before approving.

Source: Aite Group

While regulators around the globe are increasingly urging banks to adopt security at the transaction level, many FIs already had this type of defense in process in response to the threats. Three of the FIs interviewed by Aite Group indicate that they already had strong transaction-level security in place prior to the June 2011 FFIEC guidance, while 11 are working to deploy stronger technology now and one FI has stronger transaction-based security on its roadmap (Figure 5).

Figure 5: Migration to Transaction-Based Security



Source: Aite Group interviews with 16 North American financial institutions, August to November 2012.

CONCLUSION

Considering the extent to which cybercriminals study their targets and the pace with which cyberthreats are evolving, FIs need to be equally responsive in their defensive strategies. And since the bad guys don't need to make business cases to justify their innovations while the forces of good generally do, it is doubly important that FIs place their bets with the most effective technologies as they develop and evolve their layered defenses. Here are a few recommendations:

- **Don't put all your eggs in one basket.** Cybercriminals have proven adept at bypassing virtually every form of online fraud mitigation and authentication when deployed as a single point solution. To be effective in the war against cybercriminals, FIs need to adopt a layered approach that protects not only the session but also the transaction itself.

- **Multi-factor is still a good bet.** Multi-factor authentication is still a safe bet, but the approach has necessarily come a long way from the early days when it simply consisted of a few challenge questions. Today, multi-factor also implies multiple channels, blending online and mobile communication, and doing so in a secure manner that is not susceptible to known forms of compromise.

- **Continue to perform ongoing risk assessments**. It's important to stay abreast of the latest malware capabilities and understand how current defenses can (or cannot) be effective against them. To that end, make sure that your current or planned set of solutions includes the following:

    - **The ability to detect and interdict anomalous transactions.** There are often behavioral clues in the fraudulent transaction, whether it is the transaction size, the timing of the transaction, or the way in which the site navigation is being performed.
    - **HTML injection detection.** HTML injection is a common technique used by Trojans, whether they are injecting fields onto the Web page to capture credentials or injecting data to cover the evidence of their illicit transactions.
    - **Proxy detection**. Cybercriminals use proxies to mask their true endpoint and avoid potential red flags that may be raised by device fingerprinting solutions.
    - **Include the customer.** For high-risk transactions, the customer has to be included in the fight. While many FIs are wary of risk solutions that intrude upon the end-user experience, through education and partnership with the client, fraud mitigation can become a differentiator for the financial institution rather than a burden for the customer.

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
+1.517.992.5087
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:

Patrick Kilhaney
+1.718.522.2524
pr@aitegroup.com

For all other inquiries, please contact:

info@aitegroup.com