SMARTPHONES, TABLETS, AND FRAUD:
When Apathy Meets Security

Sponsored by:

Nok Nok LABS

Independently produced by:

JAVELIN STRATEGY & RESEARCH

CONTENTS

TABLE OF FIGURES

OVERVIEW

Consumers rely on their mobile devices on an ever-growing basis to keep them connected. Smartphones and tablets provide them with access to each other through email, messaging, and social media while also putting financial services and shopping in the palm of their hands. And each and every one of these activities holds value for criminals in search of account credentials and personally identifiable information (PII) to sell or misuse. Unfortunately, for all of the potential that mobile devices represent, the apathy of every mobile stakeholder is undermining the security of mobile devices and the accounts of their users. Protecting Android, iOS, and Windows mobile device users from fraud will require a concerted effort by all stakeholders to eliminate vulnerabilities, encourage security-minded behaviors, and to leverage all the security benefits that mobile devices have to offer.

KEY FINDINGS

- **Android, iOS, and Windows mobile users are undermining their security by reusing passwords more often than the average consumer.** These mobile users are about 25% more likely than all consumers to use the same password to access more than one online account. This motivates criminals to target them and their devices to secure credentials with the expectation that they will facilitate access to a variety of the victim's valuable accounts and services.
- **Heavy reliance on one-time passwords is placing Android users' financial accounts at risk.** Forty-one percent of Android users take advantage of one-time passwords (OTPs) with their financial accounts. The prevalence of mobile malware for Android capable of intercepting OTPs sent by text (i.e., Short Message Service or SMS) is contributing to the rate of fraud these users experience.
- **Mobile users prefer fingerprint authentication, which bodes well for Apple and Samsung.** Fingerprint scanning is preferred by Android, iOS, and Windows mobile users among the prevailing biometric modalities. Recent moves by Apple and Samsung to expand fingerprint-based authentication is likely to be well-received and will subsequently bolster the preference for this modality.
- **One in five or fewer Android, iOS, or Windows mobile device users are truly protecting their data from a physical intrusion.** While using a password, or better yet a fingerprint, to protect the lock screen can effectively deter some attempts to physically access a mobile device, more safeguards are needed to dissuade professional criminals. Unfortunately the use rates of remote-wipe software and disk encryption are dishearteningly low.
- **Mobile users desperately want to protect their devices from vulnerabilities in outdated OSs, but updates are not always convenient or available.** Updating the OS can be hampered by limited availability from carriers and manufacturers in the case of Android or because of how an update has the potential to undermine performance after installation in the case of iOS.
- **Android and iOS users face a significantly higher rate of fraud than the average consumer, but the reasons differ.** Users in both camps display similarly poor password and security habits, which are contributing to their risk of being victimized. More specifically, it is mobile malware that is spurring the fraud experienced by Android users, while the attractiveness of iOS users' income has placed them in the crosshairs of fraudsters.

RECOMMENDATIONS

- **Use the effective authentication capabilities of the mobile device.** To protect mobile users and their accounts from the vulnerabilities associated with the use of passwords, take advantage of hardware integrated into mobile devices to protect all channels. More secure solutions, such as those based on biometrics, can be delivered directly to consumers without the cost of providing additional hardware.
- **Encourage the use of comprehensive security software.** Comprehensive mobile security software can help prevent a variety of threats. Anti-malware capabilities can protect users from malicious apps designed to glean account credentials and other sensitive PII. Other features can include the ability to remotely wipe the device in the event of theft and notifying the user of any risky connections.
- **Be mindful of how OTPs are being used and sent.** One-time passwords sent by SMS are vulnerable to being intercepted and rerouted by mobile malware, while those delivered through email could also be stolen should the account be compromised. When using OTPs to protect valuable accounts, such as online banking, avoid sending OTPs through either of these methods.
- **Educate consumers about how biometric data is protected and used.** Fingerprint scanning benefits from its long history, including its use by law enforcement and in commercial applications and its popularity in film. Consumer concerns about the privacy and effectiveness of a biometric solution can be relieved through education, giving other modalities an opportunity to close the gaps in public awareness and comfort.

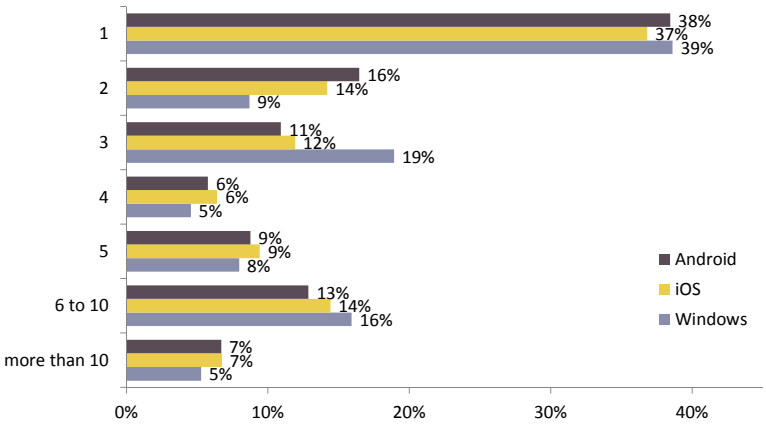
PASSWORDS: MOBILE USERS SACRIFICE SECURITY FOR CONVENIENCE

Passwords are the typical first line of defense for online accounts, and in some cases they are the only means by which an account is secured from unauthorized access. Given the breadth of available apps and services that mobile users have at their fingertips that require a password, it is unsurprising that convenience has taken a back seat to security. Mobile users have fallen into the "password trap," reusing the same passwords for multiple sites and services. As a result, they are exposing their online accounts to a greater risk of compromise and eventual misuse.

Regardless of which major operating system is being used, mobile device users are undercutting their own security at an alarming rate. More than six out of 10 Android (62%), iOS (63%), and Windows (61%) mobile device users use the same password for more than a single online account (see Figure 1). As a result, they are about 25% more likely than all consumers to reuse a password, which has repercussions for the integrity of their identities and the security of their accounts.[1]

At least 6 in 10 Mobile Consumers Reuse Passwords Across Multiple Accounts

Figure 1: Number of Online Accounts Where the Same Password Is Used, by Mobile OS User



Q61: How many of your online accounts do you use exactly the same password to access? Means number of accounts shown.

October, 2013, n varies 169 to 2028
Base: Consumers owning online accounts by mobile OS.

Password behaviors born of convenience have already motivated criminals to breach password lists, but the behavior of mobile users makes them and their devices more attractive and vulnerable targets. This in turn places the types of services delivered through mobile devices at substantial risk, including banking, email, online commerce, payments, and social media. There is a domino effect: As criminals compromise the password of an account and attempt to access it for immediate financial gain, they may also glean additional bits of personally identifiable information (PII) on a consumer and can subsequently access other accounts or defraud a user's contacts.

Passwords are cumbersome to manage, and even more so to enter on the keyboard of a mobile device. To cope with the difficulties that passwords create, mobile users are unintentionally undermining their own security. Fortunately there are effective alternatives that take advantage of the mobile devices themselves to provide ease of use and security (see Advancing Authentication section, below). Implementing these alternatives can protect mobile users and their devices in ways that passwords cannot.

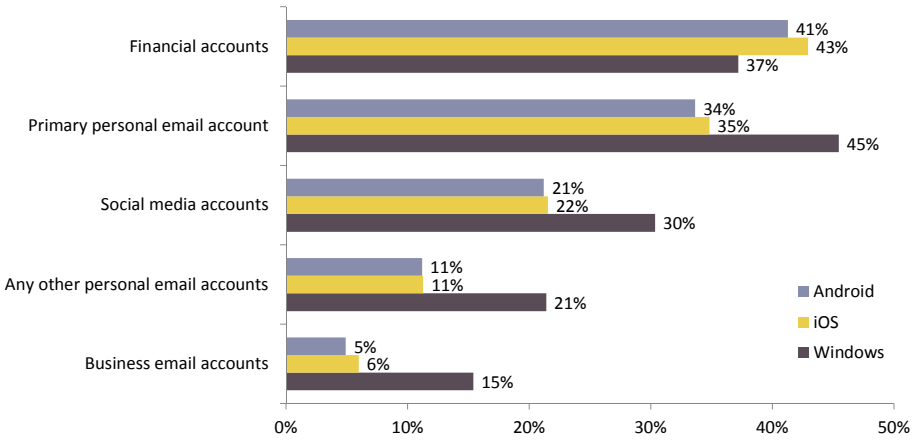
USING MOBILE DEVICES TO ADVANCE AUTHENTICATION

The love affair between consumers and their mobile devices is undeniable. But despite the allure of the latest advancements in mobile technology, consumers are accessing a variety of apps and online services using outdated authentication techniques. Ironically, mobile devices allow consumers and businesses to realize greater security by reducing the cost, and increasing the effectiveness and practicality of newer authentication technologies. Yet reaching that potential will depend greatly on the wherewithal of consumers, along with how they address implementation and use challenges.

To address the weakness inherent in traditional passwords, many online sites have turned to one-time passwords, but this solution faces its own set of challenges. Consumers may suppose that OTPs delivered through mobile devices improve the security of online services because they have become standard for two-factor authentication. Unfortunately SMS-based OTPs are being successfully targeted and compromised by mobile malware (see Mobile Threats section, pg. 12). This represents a significant threat to the integrity of any consumer's account that relies on OTPs, but in particular to the 41% of Android users who use OTPs to protect their financial accounts (see Figure 2). Greater security can be achieved by not delivering OTPs through SMS and instead using a dedicated app to circumvent the threat of malware interdiction.

More Than 4 in 10 Android Users Potentially Face Fraud Threat From Two-Factor Authentication for Financial Accounts

Figure 2: Use of Two-Factor Authentication in Online Accounts, by Mobile OS User



Q66: Are you currently enrolled in two-factor authentication for any of the following account types?

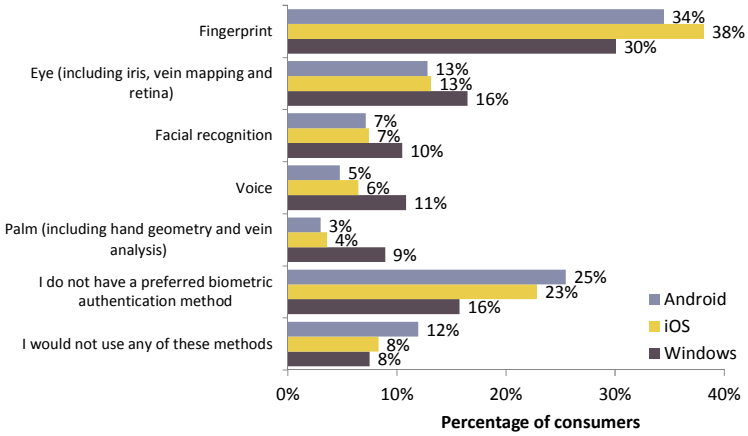
October, 2013, n varies 171 to 2048
Base: Consumers by mobile OS.

As another alternative to passwords, biometric authentication has immense promise when delivered through a mobile device. Mobile devices are uniquely suited to facilitating a wide variety of biometric solutions, including facial and voice recognition, through the use of their integrated cameras and microphones. In addition, the two largest mobile device manufacturers, Apple and Samsung, have both integrated fingerprint-scanning sensors within their flagship smartphones. The integration of all of these hardware capabilities into ubiquitous mobile devices alleviates two of the most significant impediments to the mass adoption of biometrics: user convenience and cost to deploy.

Despite the benefits that can be achieved when delivering biometric solutions through mobile devices, consumers do not value each modality equally. Indicative of their long history and the level of trust bred by familiarity, Android, iOS, and Windows mobile users most prefer fingerprint scanning (34%, 38%, and 30%, respectively) (see Figure 3). In addition to Samsung's partnership with PayPal, Apple's recent announcement of the use of Touch ID to authenticate mobile wallet transactions will have a significant effect on this trend.[2] The experience of consumers at the point of sale with this modality will further bolster trust as fingerprints replace personal identification numbers (PINs) for securing mobile wallets across a variety of devices over the long term. While fingerprint scanning has a considerable head start, competing modalities have a similar opportunity, but only if they can breed trust among consumers, especially in how they protect the privacy of biometric data.[3]

The Most Established Biometric Technology, Fingerprints, Is Preferred

Figure 3: Biometric Method Preference, by Mobile OS User



Q38: Which of the following biometric methods would you most prefer to use to authenticate your identity online?

August, 2013, n varies 112 to 988
Base: Consumers by mobile OS.

Mobile devices have changed the way that consumers communicate and interact with businesses, yet all too often these relationships are predicated on both parties' trust in rudimentary security measures. Fortunately, consumers and businesses can both derive significant security benefits from the inherent and growing capabilities of these devices. By rendering passwords obsolete, apps and online services will be less prone to fraud, no longer to be compromised by criminals with breached credentials in hand.

MOBILE THREATS: INSIDE AND OUT

Mobile devices can conveniently deliver a variety of services directly to the hands of consumers, just as they can provide another convenient avenue by which criminals can get their hands on valuable data. Highly sought-after for the commission of fraud, sensitive PII and account credentials are both stored in and transmitted through smartphones and tablets, as consumers use these devices for financial services, m-commerce, and social media. Unfortunately, the mobile security habits of these same consumers can allow criminals direct access to the contents of these devices, placing the integrity of consumer accounts and identities at risk.

Consumers face threats to the security of their devices from the digital and physical worlds. While there are some immensely pervasive threats, including malicious Wi-Fi hotspots, mobile malware, and physical intrusions, the security habits of consumers can dramatically compound the damage done when a criminal uses one of these threat vectors to compromise mobile users or their devices.

Threat:

Malicious or Unsecured Wi-Fi Hotspots

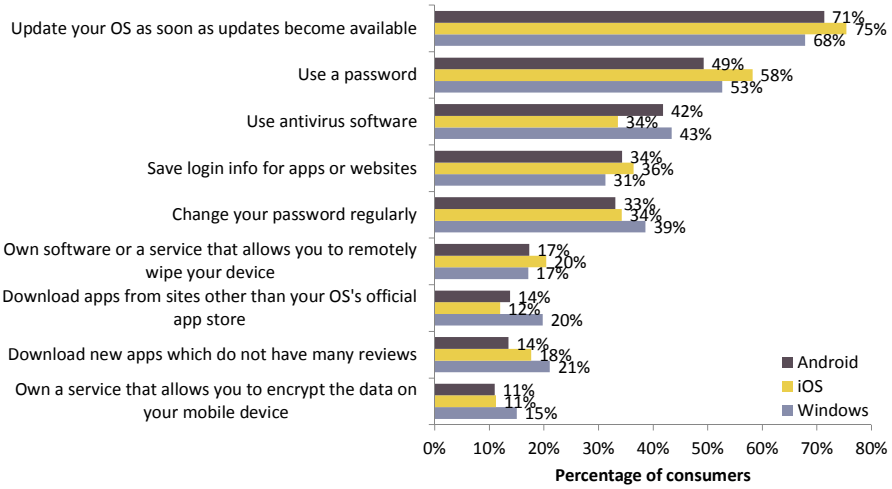
Malicious hotspots masquerading as legitimate access points provided to customers at locations such as hotels or coffee shops are designed to intercept the transmissions of connected devices. Even benign hotspots can be nearly as dangerous if left unsecured. Consumers using smartphones and tablets connected to these hotspots may have any unencrypted data intercepted, including account credentials and other PII. Even in those instances where the app or online services in use appear to be encrypted, vulnerabilities may still exist in the implementation of the encryption, exposing data to theft and misuse.

Compounding Behavior:

Consumers using Android, iOS, and Windows mobile devices all display a similar disposition to reusing passwords across multiple online accounts (see Password section, pg. 6). As a result, using a malicious or unsecured hotspot with a mobile device could expose one or more passwords to theft, potentially facilitating unauthorized access to a multitude of accounts and services.

Android, iOS, and Windows Mobile Device Users Display Similar Security Habits, With a Few Notable Differences

Figure 4: Use of Mobile Security Features, by Mobile OS User



October, 2013, n varies 171 to 2048
Base: Consumers by mobile OS.

Threat:

Mobile Malware

Millions of instances of malware and high-risk apps specifically geared toward mobile devices are being delivered under the guise of legitimate apps, through compromised websites, or through email.[4] Besides being able to access a device's internal storage, some mobile malware (such as the Bugat trojan or the mobile variant of the formidable Zeus trojan called ZitMo) can capture and redirect SMS texts, allowing criminals to circumvent authentication schemes that rely on this channel to deliver one-time passwords.[5,6,7]

Compounding Behavior:

Older versions of mobile operating systems often contain vulnerabilities that can be used by malware, but fortunately 71% of Android, 75% of iOS, and 68% of Windows mobile device users update their devices' OS when one is available (see Figure 4). Android owners can be left in the lurch, though: Whether to make an update available for a particular device is often up to manufacturers and carriers, not Google. iOS users are somewhat better off, yet updates are notorious for draining the battery of older devices, and that might discourage the practice.[8]

Unofficial app stores do not have controls as comprehensive as those of Apple, Google, or Microsoft. The result is that malicious apps are more likely to appear in unofficial stores, and the Android (14%), iOS (12%), and Windows (20%) mobile device users who are using these stores to download unofficial apps — including rogue banking apps — may each be inadvertently placing their credentials directly into the hands of criminals as a result (see Figure 4).

Security software with antivirus and anti-malware capabilities is an effective hedge against mobile device infection, yet fewer than half of Android, iOS, and Windows mobile device users (see Figure 4) are taking advantage. The iOS user responses are not completely telling, though, because iOS sandboxing renders the anti-malware capability of security apps largely ineffective, even though iOS users who choose to download third-party apps run the risk of infection.[9] Security apps can include a number of other functions, though, including the ability to identify unsecured connections.[10]

Threat:

Physical Intrusion

Mobile devices are under attack not only through their wireless connections; they also make tempting targets for criminals in the physical world. The petty theft of smartphones has placed major cities' crime rates under significant pressure, forcing calls for device manufacturers to integrate a kill switch to render them useless in the case of theft. – California recently instituted just such a law.[11] Consumers' mobile devices may also prove hard for certain personal acquaintances to ignore; familiar fraud[12] could occur when a mobile device is unknowingly used by a friend or family member to access financial services, m-commerce, or mobile wallet functions.

Compounding Behavior:

Making a mobile device inaccessible can dissuade a dishonest acquaintance from even attempting to access it in the first place. iOS users are the most likely to protect their device with some sort of password (58%), and their lock screen can be further secured by using Touch ID if they have a compatible device (see Figure 4). While some Samsung devices offer the same convenience, the remainder or mobile devices must rely on more pedestrian means of securing the lock screen. And for consumers without a fingerprint scanner who choose to rely on passwords instead, they can still be victimized by an acquaintance if they are able to glean or guess the password. This makes updating passwords regularly an

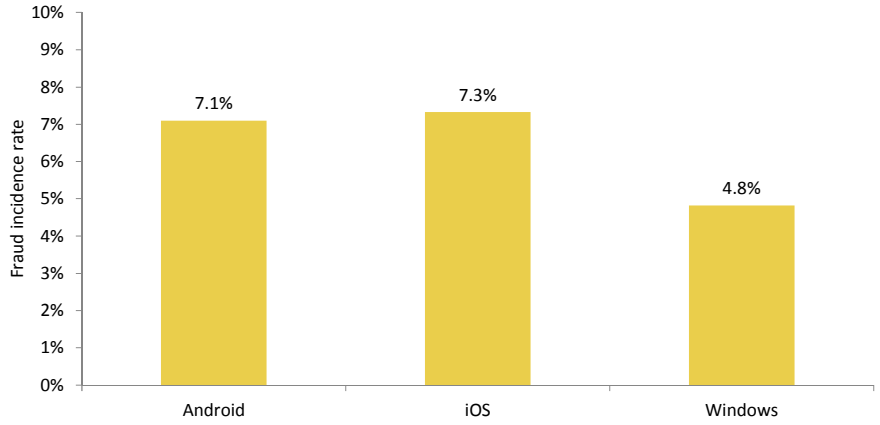
important practice, but only about one-third of Android, iOS, and Windows mobile device users update them regularly, (see Figure 4).

Securing the lock screen of a mobile device may prove to be less of an impediment to professional thieves who are intent on gaining access to the PII contained therein. In these instances, solutions that render the mobile device unattainable or unusable are more effective. Yet among all the security habits examined, these solutions are some of the least used: Remote-wipe software is used by 17% of Android, 20% of iOS, and 17% of Windows mobile device users, and disk encryption is used by 11% of Android, 11% of iOS, and 15% of Windows mobile device users (see Figure 4).

UNDERSTANDING THE CONSEQUENCES

Android and iOS Users Experience a Relatively High Rate of Identity Fraud

Figure 5: Incidence of Identity Fraud in Past 12 Months, by Mobile OS User



Q5. In what month and year did you DISCOVER that your personal or financial information had been misused? In the past 12 months

October, 2013, n varies 171 to 2048
Base: Consumers by mobile OS.

Ultimately, the multitude of threats facing mobile devices and the habits of their users are conspiring to create an environment where fraud can flourish. Not every device owner experiences fraud at similar rates, though (see Figure 5):

- Among Windows mobile device users, 4.8% experienced identity fraud in 2013, which is 10% below the rate at which all consumers were victimized (5.4%).[13] This can partially be attributed to the smaller share of the mobile device market they represent, which makes them less attractive targets, but could also be the result of other factors such as the use of non-SMS-based two-factor authentication common to Microsoft services, such as Outlook (see Mobile Authentication section, pg. 8).
- Android users face the most serious threat from malware and are placing their financial accounts at risk when relying on SMS-based OTPs for authentication (see Mobile Authentication section, pg. 8), both of which contribute to a rate of identity fraud that is 31% higher than what all consumers experienced last year (7.1% vs. 5.4%, respectively).
- Despite owning devices far less prone to malware infection than Android, 7.3% of iOS users experience identity fraud that is 36% higher than average (5.4%). This is because of their substantial market share, which makes them higher profile targets, the use of Apple services, which rely heavily on a single set of credentials, and users that have higher-than-average incomes, which make them more attractive to fraudsters.[14]

Facing significantly higher rates of fraud, Android and iOS users alike must improve their security posture if they are to have any hope of reversing this trend. While users can be encouraged to change their behaviors, some improvements can only be achieved in concert with the efforts of carriers, device manufacturers, and the businesses that use the mobile channel to reach their customers. Every stakeholder shares in the responsibility for the success — or failure — of protecting mobile devices and their users from fraud.

METHODOLOGY

2013 Identity Fraud Survey Data Collection

Javelin's ID Fraud survey was historically fielded as a landline survey using computer-assisted telephone interviewing (CATI). At the time of the survey's inception in 2003, landlines provided a relatively comprehensive coverage of the U.S. population. However, with the advent of time and technology, landline coverage has been shrinking — thus the ID Fraud survey has had increasingly less penetration into the younger, more mobile population. Cognizant of this shift, in 2011 Javelin fielded the ID Fraud survey through the KnowledgePanel®. Javelin continued to use KnowledgePanel for our 2013 ID fraud survey in order to obtain the most representative sample of U.S. adults.

KnowledgePanel is the only probability-based online panel in the U.S. Through mail, the panel recruits households with no access to Internet (at the time of recruitment) as well as cell phone-only households. The panel offers a mix of RDD-based recruitment (1999–present) and address-based sampling (introduced in 2008 and rolled out in full in 2009).

The 2013 ID Fraud survey was conducted among 5,634 U.S. adults over age 18 on KnowledgePanel; this sample is representative of the U.S. census demographics distribution, recruited from the Knowledge Networks panel. Data collection took place from Oct. 9 to Oct. 30, 2013. Final data was weighted by Knowledge Networks, while Javelin was responsible for data cleaning, processing, and reporting. Data is weighted using 18+ U.S. Population Benchmarks on age, gender, race/ethnicity, education, census region, and metropolitan status from the most current CPS targets.

Margin of Error

For questions answered by all 5,634 respondents, the maximum margin of sampling error is +/- 1.31 percentage points at the 95% confidence level. For questions answered by all 936 identity fraud victims, the maximum margin of sampling error is +/- 3.20 percentage points at the 95% confidence level.

ENDNOTES

[1] **2014 Identity Fraud Report: Card Data Breaches and Inadequate Consumer Password Habits Fuel Disturbing Fraud Trends**, Javelin Strategy & Research, February 2014.

[2] https://www.apple.com/iphone-6/touch-id/, accessed Aug. 19, 2014.

[3] **Biometrics in Banking and Payments: Versatile Voice Faces an Apple-Led Fingerprint Revolution**, Javelin Strategy & Research, January 2014.

[4] http://www.scmagazine.com/new-drive-by-download-android-malware-discovered-by-researchers/article/334475/, accessed Sept. 7, 2014.

[5] http://blog.trendmicro.com/trendlabs-security-intelligence/mobile-malware-and-high-risk-apps-reach-2m-mark-go-for-firsts/, accessed Sept. 7, 2014.

[6] http://www.americanbanker.com/issues/178_111/new-breed-of-banking-malware-hijacks-text-messages-1059745-1.html, accessed Sept. 7, 2014.

[7] http://www.informationweek.com/mobile/zeus-banking-trojan-hits-android-phones/d/d-id/1098909?, accessed Sept. 19, 2014.

[8] http://www.entrepreneur.com/article/232335, accessed Sept. 7, 2014.

[9] http://nakedsecurity.sophos.com/2014/08/22/apple-ios-malware-gets-onto-75000-iphones-steals-ad-clicks/, accessed Sept. 7, 2014.

[10] http://www.eweek.com/c/a/Security/10-iOS-Security-Apps-to-Protect-Your-iPhone-iPad-from-Hackers-492794/, accessed Sept. 7, 2014.

[11] http://bits.blogs.nytimes.com/2014/08/25/california-governor-signs-law-requiring-a-kill-switch-on-smartphones/?_php=true&_type=blogs&_r=0, accessed Sept. 7, 2014.

[12] Familiar fraud is the commission of identity fraud by someone personally known to the victim.

[13] **2014 Identity Fraud Report: Card Data Breaches and Inadequate Consumer Password Habits Fuel Disturbing Fraud Trends**, Javelin Strategy & Research, February 2014.

[14] **2012 Mobile Security: Android and iPhone Are Attractive Fraud Targets in $20B Mobile Payments Market**, Javelin Strategy & Research, November 2012.

ABOUT JAVELIN

Javelin Strategy & Research, a division of Greenwich Associates, provides strategic insights into customer transactions, increasing sustainable profits and creating efficiencies for financial institutions, government agencies, payments companies, merchants, and other technology providers. Javelin's independent insights result from a uniquely rigorous three-dimensional research process that assesses customers, providers, and the transactions ecosystem.

Authors: Al Pascual, Senior Analyst, Fraud & Security

Publication Date: September 2014

Editor Chuck Ervin

This white paper was sponsored by Nok Nok Labs. The white paper was independently produced by Javelin Strategy & Research, a Greenwich Associates LLC company. Javelin maintains complete independence in its data collection, findings, and analysis.