Trusteer

Mobility on Hold: Get Back on Track with Mobile Risk Mitigation

White Paper

*new threats, **new thinking***

Table of Contents

Mobile banking continues to gain momentum, growing faster than any other delivery channel to date. Many financial institutions contemplate expanding capabilities in the mobile channel, but they are concerned about security. Given the evolving threats, mobile innovation has outpaced the industry's appetite for deploying new capabilities.

Fortunately, new security measures are available to mitigate the risks associated with advanced mobile banking and payment features. Mobile devices must be fully protected against advanced threats. But because the key to protecting the mobile channel is to realize that it is deeply connected to the online channel, effective protection must consider risk indicators that span both channels and extend to both.

The Evolving Mobile Channel

Much continues to be written about the trajectory and the remarkable adoption of mobile banking; industry analysts estimate that over one-third of all US adults use this channel. Beyond impressive adoption statistics, the average mobile banking user logs in more than a dozen times per month.

Recent studies have shown mobile banking users to be among the most profitable banking customers. For example, last year, Zions Bank reported that online banking customers who also used mobile banking were 29% more profitable than online banking customers who did not use mobile banking. Similarly, the online and mobile banking customers had a 63% lower attrition rate than those who only banked online. Other studies have demonstrated a causal effect between customers' adoption of mobile banking and higher profitability. Whether more profitable customers tend to use mobile banking or mobile banking leads to higher customer profitability, one thing is clear: Banks must pay very close attention to mobile customers and the mobile channel.

Unfortunately, mobile banking capabilities have still not improved much beyond "online banking lite." That is, most banks continue to restrict mobile banking features to a subset of those found in online banking. A handful of institutions have begun offering mobile banking registration from a mobile device (versus requiring customers to register through online banking) and registration of new bill payees within mobile banking (rather than limiting bill payees to recipients previously registered through online banking). In addition, several banks are now offering mobile person-to-person (P2P) payments.

Providers of mobile banking and payment platforms have developed more mobile capabilities than financial institutions are willing to deploy. The institutions' reluctance stems partially from the risk of acceptance associated with any new capability, yet primarily from the risk of deploying capabilities with exposure to unknown fraud risk. Even if institutions can accurately identify security issues

associated with new features for mobile banking and payments, mitigating controls have not been readily available in the market. As a result, security concerns are stifling the growth and promise of the mobile channel. Although these concerns are valid, security technology does exist to protect new and enhanced capabilities in mobile banking and payments.

In addition to these real security concerns, several studies have indicated that mobile users continue to stay away from mobile banking and payments because of their perceived security concerns. (For more insights into consumers' perspective, see the recent reports, "Consumers and Mobile Financial Services 2013" published by the Federal Reserve Board and "Driving Value and Adoption of Mobile Payments — Consumers Want More", published by Accenture.) Financial institutions must first address the real security risks associated with the mobile channel and then address users' legitimate security concerns in order to successfully expand mobile banking and payment services.

The Mobile Threat Landscape

Financial institutions are rightly concerned about mobile threats. Cybercriminals are already employing a number of tactics in the mobile space, and they will certainly expand their attacks and attack methods. As financial institutions introduce broader capabilities for money movement to the mobile channel, cybercriminals will intensify attacks, invent new techniques, and continually challenge fraud-prevention professionals who try to keep this channel safe.

Although mobile threats fall primarily into a handful of categories, we expect the mobile channel to follow the same pattern of escalating threats seen in the online channel. The following sections examine the mobile threats utilized "in the wild" today.

Mobile Device Risks

Cybercriminals attack vulnerabilities on mobile devices to gain access to mobile banking and payment accounts as well as to online banking accounts through the mobile browser. Unlike users in the more mature online channel, users in the mobile channel are generally unaware of threats; providers of mobile platforms and applications are at the beginning stages of criminal sophistication in the mobile channel. The following mobile attack vectors are quite different from those in the online channel.

Device Jailbreaking and Rooting

Although jailbreaking (on Apple IOS devices) and rooting (on Android devices) are related, they represent different approaches to removing restrictions to software installation on mobile devices. One reason device manufacturers apply these restrictions is to improve the security posture of the device by preventing untrusted applications (in the case of Apple) or root-level access (in the case of Android) from gaining unwanted access to the device and data. Users, however, want the freedom to install applications and modify their mobile devices and are often unaware of the risks associated with jailbreaking and rooting. Hackers take advantage of the enhanced access to secretly install malicious apps and exfiltrate sensitive data.

Rogue Mobile Applications

As of this writing, Apple is approaching 50 billion total application downloads and Android is closing in at 48 billion. Cybercriminals have, of course, taken notice. Fake mobile gaming or security applications embedded with malware are routinely offered through application stores and marketplaces. Once installed, the malware can intercept sensitive information, including mobile banking credentials, or intercept SMS messages and other communication. This process of infecting and exfiltrating data is facilitated when an end user has a jailbroken or rooted device. Therefore, determining the "health" of the end user's device is a critical component of a mobile risk analysis.

Mobile Malware

Mobile devices can be infected when users access websites with exploit codes that target mobile browser vulnerabilities (e.g. drive-by downloads). As a result, a malicious application is downloaded and run invisibly so that users never see any suspicious activity. The malware can steal account access credentials or lead a user to a malicious spoofed bank site. Although we have not yet seen advanced Man-in-the-Browser (MitB) mobile malware, it is certainly just a matter of time before it appears.

Mobile Phishing

As Trusteer reported over two years ago (see blog **Mobile Users Three Times More Vulnerable to Phishing Attacks**), mobile users have a stronger tendency than online users to click through malicious links. One reason for this behavior is that the shortened URLs commonly used on mobile devices do not convey enough information to show that they are potentially malicious. In addition, mobile use ingrains the habit of quickly clicking through links, and the persistence of the mobile device means that mobile users will likely connect to a phishing site more quickly than online users (before the site is identified and taken down). Therefore, many cybercriminals target mobile users, knowing the likelihood of success is very high. Mobile phishing can lead to direct credential theft, drive-by malware downloads, or socially engineered malware installation.

Cross-channel Risks

Cybercriminals have learned that financial institutions are challenged to discover cross-channel fraud because of the siloed nature of delivery channels and their related fraud-detection systems and support organizations. The number of cross-channel attacks within the online channel at financial institutions is increasing, as are online/mobile cross-channel attacks.

Account Takeover

The primary concern in the mobile channel is a coordinated account takeover (ATO) attack that involves both the online and mobile channels. Cybercriminals steal credentials from a victim's PC via malware or phishing attacks to commit account takeover using the mobile device browser. This scheme is enabled by the tendency among banks to use the same username and password combination in both the online and mobile channels and also to use the same challenge questions as password reminders.

Depending on geography, mobile ATO attacks can unfold in a variety of ways. In the US, mobile banking via a dedicated mobile banking application or through the bank's mobile website generally does not support payments to new payees. However, criminals can bypass the mobile website and connect to the full online banking site via the mobile browser to access all features available in the bank's online banking application — including adding new bill payees. Applying security controls to the dedicated mobile application and to the mobile website but not applying those same controls to the mobile browser simply makes no sense.

Cybercriminals access accounts via the mobile channel for one key reason: mobile device ID limitations. One of the most basic authentication methods used by financial institutions in the online and mobile channels is device ID. A criminal logging in from a new device will trigger a fraud alert, resulting in limited account access or even a failed login. Mobile devices, specifically iPhones, have an interesting and potentially dangerous trait; they all look the same to a device ID system. When a user browses to a website from his native mobile browser (e.g., an iPhone with a Safari browser), the device characteristics are identical to those on almost all other iPhones: same hardware, same browser, same fonts, etc.

In this attack scheme, criminals use phishing and malware to steal credentials from victims' PCs. Remember, most banks use the same primary and secondary authentication credentials across the online and mobile channels. The criminals then log in to the bank using a mobile device and a native mobile browser (no mobile banking app is used). The bank cannot uniquely identify the device because the criminal's iPhone looks exactly like the victim's iPhone (or any other iPhone, for that matter). The criminal's login attempt will not trigger any risk indicators and a fraudulent transaction is just a matter of time. This is exactly where security silos fail.

Mobile SMS Compromise

As reported in a number of Trusteer blogs, cybercriminals have wasted no time in circumventing the mobile SMS out-of-band authentication used by many international banks. This approach involves a two-part attack, first convincing online users that they need to supply their mobile phone number to install a newly required security application on their phone. Next, users are directed to install the fake application from a link sent via SMS and enter the activation code provided by the malware. Once installed, the mobile malware captures all SMS traffic, including one-time password (OTP) codes sent by the bank to victims via SMS, and forwards them to the fraudsters. The criminals can then initiate fraudulent transfers and capture the OTP needed to bypass SMS-based out-of-band authorization systems.

Future Mobile Threats

We know mobile threats will evolve. Although we cannot yet know what future mobile threats will bring, we do know the importance of a robust, flexible, adaptable fraud-prevention platform. As in the online channel, the ability to quickly recognize changes in fraud risks and rapidly deploy appropriate risk-mitigating responses is absolutely essential in the mobile channel. Cybercriminals are able to adapt instantly, necessitating protection that can match their cunning and speed one for one.

Mobile Fraud Risk Mitigation

Because mobility introduces unique risks, a new fraud mitigation approach is essential. Protecting the mobile channel requires a holistic approach that protects against the full range of attack vectors responsible for the cross-channel and mobile-specific attacks described above. The platform must be highly adaptable to protect against quickly changing threats in this rapidly expanding channel.

Mobile Risk Engine

Based on the current threat environment, including cross-channel ATO attacks, it is clear that data across both the mobile and online channels must be considered in order to consistently and accurately identify mobile risks. The only mobile risk engine that can successfully identify all relevant risks is one that ingests risk factors for devices as well as accounts in the online and mobile channels to perform a real-time mobile risk assessment. It is important to combine these inputs to provide the highest level of mobile fraud mitigation possible. See, for example, **Trusteer Mobile Risk Engine**. Solutions that consider only one of these sets of risk factors simply cannot reliably and conclusively detect all fraud in the mobile channel.

Device risk factors are specific device-level conditions that are indicative of the overall likelihood that the device is sufficiently safe to allow access via either the dedicated banking application or a mobile browser. These conditions are discussed further below.

Account risk factors include specific session and account indicators, such as online malware or phishing detection, account transaction history, user access patterns, and user device-to-account correlation. When these factors are correlated with device risk factors, conclusive fraud detection is possible. One simple illustrative example is correlating an atypical mobile device geolocation (device risk factor) with a recent online phishing incident (account risk factor), which would be highly indicative of fraud.

Cross-channel correlation of device and account risk factors with all channel interactions and transactions allows the mobile risk engine to perform at its highest level of accuracy. Protection should be extended to all mobile banking and payment modalities, including the native mobile banking application and mobile web access. Finally, all critical transactions must be considered and protected, including payments, out-of-band authorizations, and dual authorizations.

Mobile Device-level Protection

The mobile risk engine requires device-level data to optimize risk analysis. As in the online channel, fraud prevention is far more accurate and conclusive when critical device-level data is incorporated into the fraud decisioning process. Without this data, the risk engine is incapable of accurate fraud identification, leading to missed fraud, a large number of false positives, and unnecessary customer inconvenience.

Device ID is far more challenging to generate on a mobile device than on a PC because many mobile devices appear so similar, as discussed above. However, it is possible to generate persistent mobile device identifiers by utilizing on-device software or an embedded software development kit (SDK), which uniquely identifies the device even across removal and reinstallation of the mobile app. Additionally, techniques do exist to uncover sufficient device-identifying characteristics to produce an adequate device ID, especially when other identifying session and account factors are taken into consideration.

Device risk factors may include a myriad of indicators, such as device ID, geolocation, IP address, device time, missing OS security patches, rooted/ jailbroken device status, risky system configuration settings, malware infections, and use of an unsecured wi-fi connection. Device risk data can be used to restrict functionality based on device risk level; for example, limiting specific application functions (like adding a payee or transferring money) on a jailbroken device. Typically, no single device risk factor is conclusively indicative of fraud, but when multiple device risk factors are correlated with additional account risk factors, fraud determination becomes far more conclusive. See, for example, Trusteer Mobile SDK.

Device risk factors are an important component of the mobile risk engine analysis, and they also provide device-level protection prior to such analysis. Again, whether device risk factors are taken individually or in combination, their analysis may lead a financial institution to deny account access, restrict account capabilities, or require additional authentication. Furthermore, offering end users the option of self-remediation allows the institution to better protect itself and its customers while providing exemplary customer support. For example, if the bank sees that a certain device is not running a sufficiently updated operating system version, which may indicate a poor security posture, the bank can provide a mechanism for the user to resolve these risks by following step-by-step remediation guidance provided by the mobile banking application.

It is important to reiterate that device-level protection or account-level analysis alone is helpful, but correlating these two protection layers is the only way to reliably and accurately identify mobile fraud.

Regulatory Considerations

While the industry continues to wait for mobile-specific guidance from banking regulators, it is clear that the existing Federal Financial Institutions Examination Council (FFIEC) "Authentication Guidance" (FFIEC Guidance) pertains to the mobile banking channel as well as the online channel. We do expect the regulators to eventually provide mobile-specific guidance, most likely as a supplement to the existing FFIEC Guidance. The regulators clearly stated that the guidance was a "living document" when it was released in 2005. The 2011 Supplement was the first update issued, primarily because of the increase in successful MitB attacks, which led to significant account takeover fraud losses for small to medium-sized businesses. Although a mobile-focused update has been rumored for years, the increasing deployment of mobile payments will likely prompt regulatory action sooner rather than later.

Based on the existing FFIEC Guidance, financial institutions are expected to perform a thorough risk assessment for the mobile channel and, just as important, assess cross-channel risks associated with the mobile channel. Risk mitigation controls must be implemented, including stepped-up controls for higher-risk transactions, which would certainly include transactions that involve money movement into or out of the financial institution.

The current FFIEC Guidance also requires financial institutions to implement continuous risk assessment and implement multiple security layers to detect fraudulent transactions. A mobile risk engine detects high-risk activity by assessing the risk of every mobile device, mobile login, and mobile transaction. The risk-based recommended actions can include reauthenticating the user and preventing access to certain transactions or the account.

Summary

The mobile channel is clearly becoming an increasingly strategic component of the bank customers' experience. However, security concerns have justifiably delayed the introduction of more advanced mobile capabilities because bankers fully understand that any missteps in the mobile channel could be catastrophic to adoption and usage by consumers and businesses. Protecting this channel against current and emerging threats is critical to its acceptance, adoption, and full growth potential.

The risk of mobile fraud is a key component of an institution's overall fraud-prevention strategy. The time is now to develop and implement strategies to mitigate the risks of mobile fraud and to integrate these capabilities with the institution's overall fraud management platform. The best way to detect current and future fraud schemes is through an integrated, adaptable mobile risk engine. Getting mobile banking and payments back on track is easy once the path becomes clear.

About Trusteer

Boston-based Trusteer is the leading provider of endpoint cybercrime prevention solutions that protect organizations against spear-phishing, and advanced malware that enable targeted attacks and data breaches. Hundreds of organizations and millions of end users rely on Trusteer to protect their managed and unmanaged endpoints from online threats and advanced information-stealing malware. For more information please visit: **www.trusteer.com**.

Trusteer Inc.
545 Boylston Street, 5th Floor
Boston, MA 02116
T: +1 (866) 496-6139
T: +1 (617) 606-7755
info@trusteer.com

trusteer.com

Trusteer