SECURITY AND AUTHENTICATION IN FINANCIAL SERVICES

A Mercator Advisory Group Executive Brief Sponsored by IDology

February 2016

Mercator Advisory Group recently interviewed fraud management executives at financial services institutions to evaluate the challenges of identity verification and deterring online and mobile-based fraud. These FIs offer an array of consumer banking products ranging from checking and savings accounts to credit cards, personal loans, person-to-person (P2P) payment services, and financial management tools. Conclusions drawn from these interviews are summarized in this Executive Brief.

The Rise of Mobile as an Important Channel for Everyday Financial Activities Is Creating New Challenges

There is no doubt that cyberfraud management and identity verification are top concerns in financial services, as consumers shift more of their financial activities online and to the mobile channel. The head of digital channels for a community bank commented, "Fraud is going up in all channels—mobile and online." This was corroborated by IDology's 2015 Fraud Report, which saw an increase in overall suspected fraud attempts for a third year in a row – 36% in 2013, 40% in 2014, and 46% in 2015. Not only are customers using mobile for everyday activities like checking an account balance, transferring funds, and reviewing transaction history, but even the account opening process is moving to mobile. Some of the executives interviewed mentioned that they had plans to offer mobile-based account opening within the next two years and doing so is just a question of getting the necessary capabilities ready. An executive from an online-only bank that has made significant investment in offering a best-in-class mobile experience said that onboarding via mobile device is almost preferable to onboarding via the desktop Web channel since mobile devices provide a rich set of data on the user including geolocation tags, device ID, and SIM identifiers.

Mercator Advisory Group's CustomerMonitor Survey Series finds U.S. consumers' increasingly turn to their mobile devices as a replacement for other banking channels.

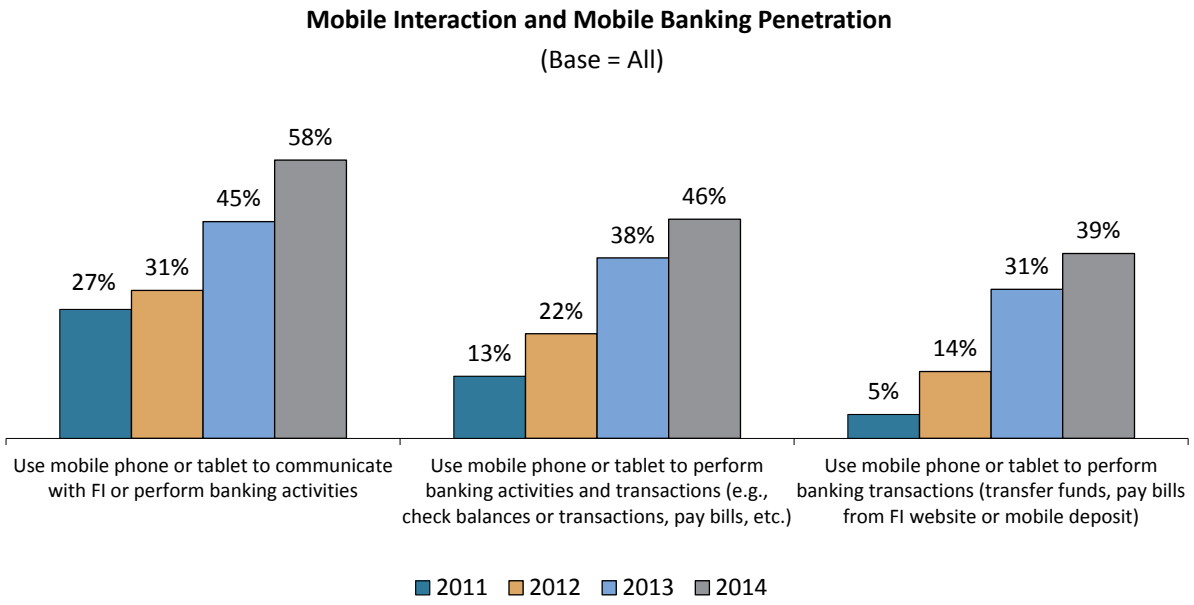

Figure 1. Source: Mercator Advisory Group CustomerMonitor Survey Series, Banking and Channels, 2011–2014, Question 56

Nevertheless, the migration to mobile presents unique challenges for financial institutions. With respect to security, mobile devices have many nuances fraudsters can exploit—from the millions of change events (for instance phone number or carrier changes, and device upgrades) to mobile technology attack methods such as mobile spoofing, cloning, and hacking. Attaining a good customer experience and ease of use in the mobile environment also present challenges for financial organizations. Especially in the account opening process, the screen size limitations of the mobile phone mean that FIs have to be judicious in how they collect personally identifiable information while still maintaining usability and security. More than one executive interviewed for this study highlighted the importance of looking deeper into mobile device attributes in this regard, for example by being able to access mobile phone attributes through real-time access to the network and carrier information to establish mobile identities or to match location data with other key data points about the user in a way that is seamless and user friendly.

Willingness to Experiment with New Forms of User Identity Verification

Fraud prevention for online and mobile banking requires more than username (user ID) and password based authentication. Among the authentication approaches being evaluated by financial institutions are Touch ID fingerprint, voice recognition, facial recognition such as photoID scanning and validation with face-matching capabilities, email verification, improving knowledge-based authentication with more sophisticated questions that can't be answered on social media, and one-time passwords. Adding multiple layers of authentication to augment user ID and password seems to be the approach that most FIs have adopted. Using this approach, financial institutions can better control the user experience by deploying these additional layers as needed, thus reducing the number of friction points. When evaluating biometrics, financial institutions recognize that fraudsters can find ways to spoof fingerprints or voices or claim to be the legitimate customer when they are not. Therefore, other methods of identity verification are needed to supplement biometrics.

> *"We are getting away from using user ID and passwords and moving more toward biometrics as a better way to verify identity."*
>
> –CIO, a Top 25 Bank

Most FIs now realize that they need different procedures and practices when customers access their services by mobile device. Executives in the FIs surveyed seem divided on what the best approach for enhancing their user authentication processes might

be, with some preferring voice and facial recognition while others advocate for using fingerprints through Touch ID. "We would also like to get voice recognition—another feature that would be better suited for mobile devices than computers because many desktops don't have microphones. We like the biometrics because it causes less customer friction, but I think we'll get complaints even with voice recognition," commented the SVP of Digital Channel Management at a leading bank. In part, the focus on identifying new authentication methods is being driven by the need to improve user friendliness in mobile banking.

> *"Our customers want us to be secure, but they hate to have to register for their devices—though we as a bank are not changing our minds about the registration process. We've done some customer surveys and their number 1 complaint for online banking is why do we have to send back the codes before we can gain access. It's a pain in the neck. Someone wrote in the comment section, "I really like security, but I hate having to put up with it."*
>
> –SVP, Digital Channel

These user identification processes are being used in conjunction with CIP, location indicators, activity indicators, device indicators, and other tools to detect and fight fraud, such as a collaborative fraud network.

Account Opening of Particular Concern in Fraud Management

The account opening process has historically been associated with the greatest fraud risk in a customer life cycle. The first 90 days is when fraud is most likely to occur, and therefore new customers receive extra scrutiny. The Director of Risk at the online-only bank cited above gave additional insight into one form of this early stage fraud by saying, "ACH origination fraud is always a big issue. Since most customers load their accounts through ACH transfers, monitoring these transactions and locking those accounts that may have funds from compromised sources quickly is very important. ACH origination fraud went up sharply a year ago and we had to temporarily suspend onboarding. [The bank] has been continuously improving its fraud monitoring techniques to address this issue." Unless a customer's account has been compromised, it is rarer for a "normal" customer who has exhibited regular patterns of activity to suddenly go "rogue." This again highlights the importance of flagging suspicious accounts at the very beginning of the customer life cycle. However, FIs have also reported an increasing number of "false positives," instances win which legitimate customers are being turned down by the FIs' fraud detection software. Striking the right balance is a high-priority.

In fact, financial institutions' turn-down rates have been rising, in part as a consequence of fraud prevention tactics. This is a sign that banks need to improve their identity verification processes by implementing a layered approach that escalates to various levels of verification based on risk profile as well as implementing new forms of verification such as facial scanning or other data sourcing to minimize the false positives. When customers register online or by mobile, the consumer may not always have all the information needed to complete the registration. The Chief Information Officer of a regional bank remarked, "We use common know-your-customer verification processes and run the results to match our databases. If we can't verify their identity, then we ask for additional information. We evaluate a number of criteria." By looking deeper into the data and evaluating consumers through multiple layers, FIs are able to create a frictionless experience for legitimate consumers but can escalate authentication to the next level if potential fraud flags are present.

When financial institutions' processes result in turning down legitimate account appliants, there is a compelling opportunity to improve business processes, enhance identity verification methods, and automate processes to provide better authentication, reduce customer friction, and thereby expand the customer base.

Financial services constantly require updating of customer data. As one executive remarked, "The hardest part of the identity verification process is the ability to truly match. Our inability to match accurately can result in more fraud." Proper identity verification requires much more than just matching to data sources, especially when accounts may come from compromised sources. Compromised sources need to be identified immediately and locked. Identification involves analyzing more than data—it includes identity attributes. activities, geolocation, device attributes and ownership, and use of the device itself in real time in

order to evaluate the risks and dynamically escalate only the accounts at risk to higher levels of authentication. Developing a unique mobile identity based on multiple mobile-specific and identity attributes most indicative of potential threats that, once verified, moves with the individual across platforms is valuable. It also reduces friction for the customer when that person changes carriers or mobile phones. It supports more secure transactions in a positive, friction-less environment.

Vendor Reliability and Ease of Integration Are Most Desired by FIs

Fraudsters are innovative, finding new tactics for gaining information to disguise their identities for financial gain by using event changes or new forms of spoofing, hacking, or account takeover. Financial institutions must be nimble enough to adjust their authentication processes to combat these new tactics with customizable solutions, not just static scorecard fraud monitoring software. Customizable solutions offering greater depth of information sourcing and analytics are needed that enable FIs to develop and adjust their own scoring systems with multiple tiers of analysis to reflect changes in their environment in order to combat these new fraud attack techniques. Situations that may be low risk to one financial institution may be higher risk to another, and risk may also depend on the time of year or the type of account. Fraud monitoring tools allow such customized processes to be applied even within an organization to address the nuances of different types of customers or services.

When a financial instiution os evaluating a vendor's mobile' based identity verification and fraud management solutions, ease of integration is a critical attribute. The solution must be robust and customizable as well. And the vendor should have a proven track record and financial stability. There also has to be a clear return on investment, or ROI, that justifies the investment in a new solution. One executive interviewed characterized the vendor selection process this way: "The key factor when we select a fraud monitoring vendor is to evaluate to what extent the solution helps us to reduce fraud, how much less fraud would we have if we bought it. I'd like to give them our entire database and let them run it—show us that you can identify more fraud than we can ourselves and then compare that with the cost of the product. If it reduces 10% of our fraud but costs a million dollars, that won't fly."

Customer service was another key attribute in vendor selection that was highlighted by the financial service executives interviewed for this study. One executive mentioned the need for the financial institution to be able to support the vendor's solution on its own and not have to direct the end customers to a third-party support team. In any case, financial institutions do not want to turn away legitimate customers because their fraud procedures are too cumbersome or intrusive. The solution should not cause too much customer friction.

Conclusion

Americans are spending a growing share of their digital time on mobile. According to recent data released by KCPB, adults in the United States spent 5.6 hours per day on their mobile devices in 2015, an amount of time that has grown at a compound annual growth rate of 10.98% since 2008. Financial institutions are scrambling to offer consumers mobile access to their products and service that is comparable to access available via the online Web available through the desktop computer since this is the experience consumers have come to expect. This shift to mobile has placed financial institution's security and authentication needs in a state of flux as the FIs experiment with new ways of delivering banking services securely through the mobile channel. In addition, each financial institution has its own unique view of risk and requires solutions that can be customized to fit its risk management governance model and often individual product risk profiles.

Financial institutions recognize that they need more sophisticated fraud management and identity verification processes than user ID and passwords alone. Biometric identification through fingerprint, voice, and facial recognition is of growing interest as a way to balance security with improving the user experience. However, biometrics tends to come later in the fraud detection value chain. Early in the process, financial institutions need to be able to balance the need for enhanced risk processes with the all-important customer experience. Creating too much friction in the account acquisition or onboarding process is uncompetitive,

as financial institutions know. What they need is thus multilayered authentication workflows that allow them to apply rules in a logical manner that prevents unnecessary input or verification steps. Mobile is also opening up new tools to fight fraud, as these devices come with a range of sensors that allow a much deeper understanding of who the user is (i.e., the user's identity and patterns of behavior). FIs are looking to build capabilities that address this aspect by investing in solutions that leverage geolocation, for example, and other relevant data.

The increased sophistication of cutting-edge software solutions to fight fraud brings financial institutions the opportunity to use these tools to build mobile identities with carrier data for their account holders. By creating a more nuanced and complex identity, one that incorporates personal, device-dependent data and location data into a comprehensive view, will allow financial institutions to provide a far more seamless experience for the "good" consumer and allow faster and more effective identification of fraudulent account activity.

About Mercator Advisory Group

Mercator Advisory Group is the leading independent research and advisory services firm exclusively focused on the payments and banking industries. We deliver pragmatic and timely research and advice designed to help our clients uncover the most lucrative opportunities to maximize revenue growth and contain costs. Our clients range from the world's largest payment issuers, acquirers, processors, merchants and associations to leading technology providers and investors. Services include *Banking Channels, Credit, Commercial and Enterprise Payments, Debit, Emerging Technologies, Global Payments,* and *Prepaid practices*, which provide research documents and advice; *CustomerMonitor Survey Series*, which report and analyze primary data collected in our biannual consumer surveys; and *Consulting Services*, which enable clients to gain actionable insights, implement more effective strategies, and accelerate go-to-market plans; offerings include tailored project-based expertise, customized primary research, go-to-market collateral, market sizing, competitive intelligence, and payments industry training. Mercator Advisory Group is also the publisher of the online payments and banking news and information portal PaymentsJournal.com. Visit www.mercatoradvisorygroup.com.

About IDology, Inc.

IDology, Inc. provides innovative technology solutions that verify an individual's identity and/or age for organizations operating in a customer-not-present environment. The IDology platform serves as a collaborative hub for monitoring and stopping fraudulent activity across the entire network while also driving revenue, decreasing costs and meeting compliance regulations.

Founded in 2003, IDology offers a solution-driven approach to identity verification and fraud prevention, providing streamlined processes that ultimately help increase customer acquisition and improve the overall customer experience. IDology has developed an on-demand technology platform that allows customers to control the entire proofing process and provides the flexibility to make configuration changes that are deployed automatically – without having to rely on internal IT resources or IDology's customer service – so customers can stay ahead of the fraud landscape while also maintaining compliance. Visit https://www.idology.com/