DEPTH. FOCUS. SERVICE.

MERCATOR ADVISORY GROUP

SECURITY CHALLENGES IN DIGITAL CHANNELS: FRAUD PROFESSIONALS WEIGH IN

A Mercator Advisory Group Research Brief Sponsored by IDology

March 2016

CONTENTS

Executive Summary

With the rise of digital channels (online and mobile), the landscape of customer communication and sales across industries is rapidly changing and with it the related risks of data breaches and fraud. In light of the rapidly evolving fraud risk, Mercator Advisory Group was commissioned by IDology, Inc. to research fraud prevention techniques and strategies used in various industries by interviewing fraud management executives in four industry verticals—financial services, alternative financial services, healthcare, and insurance. This Mercator Advisory Group Research Brief provides an overview of these findings. For information specific to each of these industry verticals, see the four separate Mercator Advisory Group Executive Briefs sponsored by IDology: *Security and Authentication in Financial Services, Security and Authentication in Alternative Financial Services, Security and Authentication in Healthcare,* and *Security and Authentication in Insurance*.

While each industry faces unique challenges and opportunities in terms of fraud vectors and fraud prevention, Mercator's primary research conducted through interviews with fraud management executives revealed certain commonalities across industries. Among the key findings of the study are the following:

- The growing number of data breaches in the United States is increasing the ability of fraudsters to gain identity information and account access information—and creating new risks for service firms.
- Multilayered authentication protocols are critical for assuring the success of identity verification and fraud management strategies as well as preserving a positive user experience for customers.
- Mobile account acquisition, opening, and self-service are important focus areas for investments in fraud management technologies.

Introduction

Fraud is an evolving risk that cuts across all industries and technologies. While companies develop increasingly multilayered and innovative security and fraud management solutions, fraudsters are equally adept at shifting strategy and discovering new methods to attack sensitive personal and financial data. In the ongoing battle to fend off fraudsters, companies are at a significant disadvantage. That is because they have to ensure that their products and services are customer friendly and avoid any noticeable customer friction that is likely to induce the consumers who are end users to look to competing providers.

Historically, companies have used indirect sales and communication channels to interact with potential and existing customers. In recent years, these have included digital channels (mobile and online). Organizations can reduce costs to the consumer through the use of digital channels, but the rise of digital channels has resulted in a new "front" in the cybersecurity battle. Today, companies in many industries are struggling to balance security and authentication with the need to deliver a customer-friendly experience with minimal friction.

Data Breaches and Social Engineering

The shift to more electronic records and payments means that a greater share of sensitive personal and financial information is stored remotely. With this shift, the potential for breaches of security systems has grown in the past few years and there have been a number of notable data breaches across industry categories. Within the healthcare industry alone, in just the first five months of 2015, data breaches occurred at three major health insurers in the United States—Anthem, Premera Blue Cross, and CareFirst—affecting up to 92 million patient records. The growing number of data breaches is significant. Identity fraud can ruin the victim's credit when bills remain unpaid and importantly, across many industries, companies have not come to grips with the potential consequences. Medical personnel, for example, often underestimate the potential for identity theft since an in-person visit by the consumer is required for most prescriptions and treatments. Once they have hacked patient records, criminals can use the stolen identity or insurance information to obtain healthcare themselves, acquire prescription drugs for resale on the black market, sell the insurance information to uninsured persons or develop other schemes to perpetrate fraud such as creating a fake clinic or facility to sell but never ship medical equipment reimbursable by a health insurer or Medicare/Medicaid.

The threat is not limited to healthcare. Companies involved in alternative financial services, for example, have found that social media and email can connect fraudsters to unsuspecting consumers and help drive "social engineering" scams in which fraudsters trick victims into divulging their credentials. This fraud type is particularly concerning given that once criminals are in possession of valuable account credentials, it is more difficult to stop them until a loss has been incurred. Commenting on this issue, a VP of Risk Management at a leading alternative financial services provider said:

> *Identifying the person speaking or registering is our number one priority. If we give approval to the wrong person, then everything down the road can go wrong and we've opened up a big pool of fraud—unauthorized charges, charge-backs and Better Business Bureau inquiries."* *–VP, Risk Management, Alternative Financial Services Provider*

For companies providing alternative financial services and indeed, for any companies that handle sensitive personal and financial data of their customers, the impact of a significant data breach could be devastating. Consumer trust wanes with each breach, and the brand suffers. Lack of consumer trust resulting from repeated breaches at a company could damage a company's reputation and lead to its downfall. To counter these potential risks, companies of all kinds are paying attention to and, more important, making investments in improving their security systems. Brand reputation is a factor that firms are very much aware of in deciding to modernize their systems, as seen in the following quote from a Chief Privacy Officer at a healthcare company:

> *". . . We strongly believe that the extra finances and effort in dealing with preventive measures for fraud and compliance are minimal compared to the expense of dealing with the harm to our consumers and the organization, the brand damage that occurs in putting out the fires when an organization is faced with fraud and breaches."*
>
> *–Chief Privacy Officer, a Healthcare Provider*

Multilayered Identity and Fraud Management

As security measures are increased, fraud prevention protocols have changed from simple username (user ID) and password-based authentication to procedures that include technologies like Touch ID fingerprint, voice recognition, facial recognition such as photo ID scanning and validation with face matching capabilities, and email verification, among others. To be truly successful, authentication strategies should be based upon multiple ID validation methods and the applicant's prior behavior and device profile, as well as monitoring usage patterns after customer registration. Furthermore, over the course of the interviews for this study, Mercator Advisory Group discovered that many providers know they need to improve identity verification and fraud prevention. They understand that adding new layers in the workflow minimizes friction by escalating to higher levels of validation when there are potential fraud indicators.

Across industries there is a clear desire to develop omnichannel strategies. Within the insurance industry, for example, companies understand that the historical agent model must be adapted to changing consumer preferences. The agent-based model has a number of engagement points with the consumer, whereas the direct channel, with its online- and mobile-based onboarding and customer service, is widely considered to be less expensive but very competitive although it requires additional investments in technical, operational, and business process infrastructures.

No channel is immune to fraud, and consumers or even agent brokers can disguise their identity and cause fraud losses, such as through misuse of brokers' Internet Protocol (IP) addresses. But many larger insurers invest heavily in sophisticated back-end authentication to verify customer identification, as well as device fingerprinting with required registration of devices used for communication and transactions, thus highlighting the commitment to multilayered identity and fraud management solutions. Commenting on cyberfraud, one marketing executive for a major insurer told Mercator:

> *"Cyberfraud is a green field—it's not mature yet and we're still trying to figure out how to deal with it. We are not confident we understand the variables and the processes we need to implement the solutions and mitigate the risks."*
>
> *–Marketing Executive, a Major Insurer*

Although willingness to commit to multilayered identity and fraud management solutions is present across industries, industry executives interviewed for this study made sure to note that not all solutions are created equal. Customizable solutions that offer greater depth of information sourcing as well as analytics that enable companies to develop and adjust their own scoring systems with multiple tiers of analysis are more valued because they provide a more precise, surgical approach to combatting fraud.

No matter how innovative a solution might be, though, ease of integration is critical. According to participants in this study representing a range of industries, their companies seek robust, customizable mobile-based identity verification and fraud management solutions. Other key attributes include a vendor's having a proven

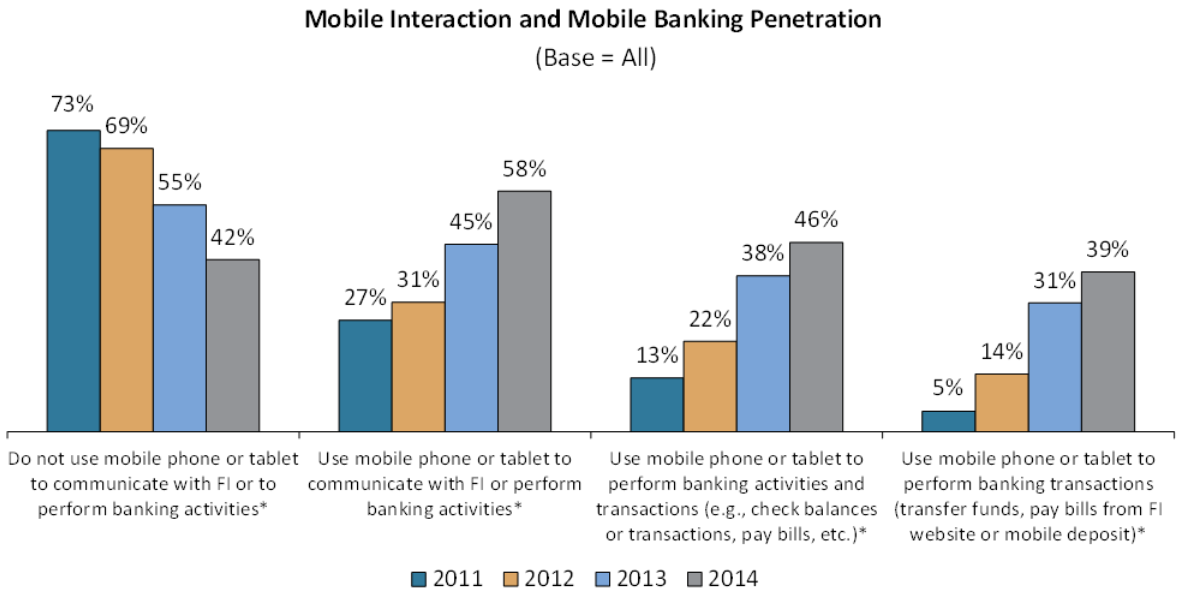
track record and financial stability. There also has to be a clear return on investment (ROI) for the new solution that justifies the investment in it. For providers of fraud prevention solutions, these attributes and performance metrics are critical, and these criteria highlight the reality that delivering effective fraud solutions is not straightforward, despite the demand.

Mobile Account Management

Increasingly, consumers are using their smartphones or other mobile devices for everyday activities like checking account balances, transferring funds, and reviewing transaction history. Even the account opening process is moving to mobile. While not yet available at every financial institution or alternative financial institution, mobile account opening is a feature commonly cited as the next "must have." According to executives interviewed in this study, institutions that do not offer mobile-based account opening today plan to do so within the next two years.

This investment appears worthwhile given changing consumer preferences. According to Mercator Advisory Group data from its CustomerMonitor Survey Series, in 2014, 58% of the 3,000 U.S. adult consumer base indicated they used their mobile device to perform general banking activities, and a further 46% indicated they use their mobile device to complete select banking and payment transactions. Figure 1 presents Mercator's survey data on the historical usage of mobile devices for banking transactions in the United States.

Figure 1: U.S. Consumer Mobile Interaction and Banking Penetration



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

The migration to mobile presents unique challenges for companies. When it comes to security, mobile devices have many nuances that fraudsters can exploit, from the millions of change events (for instance phone number or carrier changes, device upgrades, and more) to mobile technology attack methods such as mobile spoofing, cloning, and hacking. User experience and ease of use in the mobile environment are also challenges for organizations simultaneously trying to maintain device and transaction security.

Likewise, with mobile account opening, fraud is a potential serious consequence. According to the interviews in this study, the account opening process has historically been associated with the greatest fraud risk in a customer life cycle. In financial services, the first 90 days of an account is when fraud is most likely to occur and is therefore the time period when new customers receive extra scrutiny.

Although mobile account opening can reduce costs across all industry categories, providers have to balance the positive consumer experience of this convenient process with the increased risk of fraud. This is highlighted by a quote from a high-level executive at a well-known financial institution:

> *"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 one 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 Management, a Financial Institution*

Mobile security need not be a point of friction. Biometrics, along with user identification processes like location indicators, activity indicators, device indicators, and other tools to detect and fight fraud represent the next generation of security and authentication while offering a superior customer experience.

Conclusions

Fraud is always evolving. Prevention requires continual upgrade and improvement of security systems to ensure that sensitive personal and financial data is protected. The growing use of mobile devices as a consumer entry point has led to more data compromises and account takeovers via digital channels.

While mobile and online channels are increasingly targeted by criminals, the fast-growing consumer adoption of these channels has resulted in industry attention and investment in the channels and in digital security. As result, companies have moved to incorporate fraud management as a competitive feature of their service offerings, and to develop relationships with customers in order to develop trust and to generate sufficient customer data to help enable better security over the long run.

With more customer interaction moving to digital channels every day, sophisticated platforms must be created with flexible rules and protocols to ensure that the number of false positives is limited and that the customer experience is not negatively impacted. Furthermore, these systems must be able to adapt to a shifting number and variety of data inputs and can collect information across a number of channels, while ensuring positive customer interaction and bringing a strong return on fraud prevention investment.

Copyright Notice

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/