# SECURITY AND AUTHENTICATION IN ALTERNATIVE FINANCIAL SERVICES

*A Mercator Advisory Group Executive Brief Sponsored by IDology*

**February 2016**

***Mercator Advisory Group recently interviewed fraud management executives at alternative financial services organizations to evaluate the challenges of identity verification and deterring online and mobile-based fraud. Each of these firms sells general purpose, open-loop prepaid cards, and ancillary services such as person-to-person payments (P2P), bill payments, and short-term loans. Conclusions drawn from these interviews are summarized in this Executive Brief.***

## Alternative Financial Services Create New Channels for Consumers—and Criminals

Payment fraud and identity theft are also benefiting from the technology innovations creating new, online channels for account acquisition and customer service. Despite businesses' greater investment in security and stricter enforcement protocols, fraudsters are discovering new ways to disguise their identity and steal other identities such as through new spoofing or phishing attacks. Payment industry executives realize that as EMV chip technology is implemented in the United States to combat counterfeit card fraud, attacks on online and mobile channels will become more frequent. Evidence suggests they are right, since widespread adoption of EMV worldwide has led to an increase of online and card-not-present fraud globally. The task of protecting digital channels has therefore become even more urgent.

Cybercriminals tend to follow the path of least resistance, and the new market segment for alternative financial services (AFS) is one that offers the potential for a higher rate of return for them in the short term. In this Executive Brief, Mercator Advisory Group looks at risk management practices and fraud potential in new AFS business models, with a focus on two—marketplace lending and prepaid, reloadable accounts. We consider some of the business drivers that expose these types of companies to increased risk and discuss some of the best practices and technical solutions being deployed to combat fraud.

A primary reason the AFS segment was considered important for this study is the significant amount of capital being invested in growing this market, approaching $1.5 billion in the U.S. alone. This level of investment activity will motivate the market to expand rapidly, but because the segment uses an online-only channel strategy, the success of expansion will depend on user trust. Loss of trust could have a lethal impact on these businesses. For many of these companies, the necessity of user trust extends beyond consumers. Marketplace lending platforms depend on investments from individuals and institutions to fund their loans, but those investors will only fund loans if they have a high degree of confidence that the borrowers on the platform are legitimate consumers and not fraudsters.

Prepaid cards used in lieu of traditional banking accounts are another market growing at double-digit rates. Nearly all prepaid card programs support online account application and online account management services such as loading funds, bill payments, access to account balances, transaction history, and online alerts. Now these same companies are launching sophisticated mobile

apps to enable real-time alerts, remote check deposit to prepaid cards, person-to-person (P2P) payments, and real-time bill payments. All of these tools offer value to consumers, but they also are valuable to cybercriminals looking for opportunities to break into accounts.

## Managing Fraud Risk in a Virtual World

One of the challenges the alternative financial services market faces is the lack of empirical fraud data related to the new kinds of lending channels to guide their fraud management. Forging new channels means that the inherent risk that follows may not be well rationalized. Even in a market like prepaid, which is arguably the most mature of this segment, executives concur that instances of both online and mobile fraud are becoming more frequent. Much of that fraud exploits vulnerabilities in the methods used to establish customers' identity in a digital account acquisition environment. "Authentication is becoming more challenging in general, given the increased prevalence of compromised data," commented a VP of Risk Management.

> *"Mobile is so new that we are just testing the waters. We want to make sure we have additional layers of security with device fingerprinting before we really push mobile."* –Director of Fraud Management

Applying for a financial account online is now commonplace, but few vendors allow mobile-based account applications. "We assume mobile users access our website, but it's not that easy to register by mobile," noted the Chief Information Officer of one AFS provider. One provider found that just six months after launching an app that enables mobile-based account application, mobile represented 1 in 4 applications the company was accepting. Since volume of transactions is greater online than by mobile, prepaid vendors currently see more fraud online than by mobile, but they are nonetheless investing in more sophisticated antifraud features in anticipation of rapid growth in the mobile channel.

Fraud mitigation in this new world does not just include post-account-acquisition activities. Rather, it has to be designed in such a way as to ensure that the individual opening an account and accessing the services is the same person each and every time. User authentication is not simply a function but is a cornerstone of the value chain and can be achieved through process flows that incorporate biometrics, knowledge-based authentication (KBA) questions, device imprinting, and ID data. In other words, single-factor authentication is wholly inadequate in today's risk environment. The industry is at the inflection point where multifactor authentication is the de-facto standard and "step-up" authentication will soon be the norm.

One of the issues facing AFS providers is the problem of balancing customer friction against false positives. In our study, we spoke to one provider who reported declining roughly 50% of all registrations because of suspected fraud and being concerned that not all of these were, in fact, fraudulent. This kind of problem can be addressed effectively by using multiple layers of authentication in the acquisition workflow and escalating to higher levels of identity verification based on a registrant's risk profile. By using a scalpel instead of a sledgehammer in the user authentication protocol, a financial services provider can approve legitimate consumers with minimal friction or escalate the authentication, only if necessary, for further review. This enables AFS providers to reduce false positives as well as to automate some manual review processes. The importance of real-time authentication cannot be understated since consumers applying for loans or accounts online or via mobile channels have the expectation that their application will be decisioned while they wait.

## Common Types of Fraud Using Prepaid Cards

"Identity theft issues are the biggest area of fraud for us, and much of it involves tax refunds," remarked a Chief Information Officer. Fraudsters steal a taxpayer's identity and file a tax return in the person's name requesting that the person's tax refund be loaded onto a prepaid card, an option offered by the IRS.

Social media and email can connect fraudsters to unsuspecting consumers. Another common fraud type is victim-assisted fraud or "social engineering" scams in which fraudsters trick victims into divulging their credentials. A fraudster may pose as a bank or a law enforcement officer and request that the victim purchase a reloadable card for payment of a fee or fine. One prepaid

vendor reported having eliminated requiring a PIN access code for card loads because a PIN could easily be divulged to a fraudster by a victim. PIN access was replaced with swipe loading using ACH rails, since ACH has its own validation and customer authentication process to deter criminals. Even if victim-assisted fraud does not pose a direct loss for the provider, no one wants the negative publicity associated with this type of fraud.

Driving this kind of fraud is the widespread availability of "perfect identities"[1] on the "dark Web," which are leveraged by fraudsters to defraud tax agencies, open financial accounts, and secure loans.

> *"Identifying the person speaking or registering is our #1 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

Thus, the account registration or application process poses the greatest risk of fraud for alternative financial service providers. That is because once criminals are in possession of valuable account credentials, it is more difficult to stop them until the loss has been incurred. Registration typically involves a series of processes built around varying degrees of rules or scoring-based logic and company risk policies used to validate an account applicant's identity. Providers have a degree of latitude in the way they approach the validation. Most use multiple layers of authentication at registration and step-up authentication at different points of customer engagement. However, as AFS providers develop new technology solutions and gain expertise to successfully mitigate some forms of account takeover, fraudsters will evolve in tandem and shift their attention to less well-defended channels. In particular, mobile devices now provide criminals with new means by which to compromise the consumer data that is stored or transmitted by those devices, thus opening additional pathways to lucrative account takeovers.

Authentication strategies can be based on using multiple ID validation methods, the applicant's prior behavior, and the device profile as well as monitoring usage patterns after cardholder registration. We found providers concur on needing to improve identity verification and fraud prevention by adding new layers in the workflow to confirm that customers are who they say they are and to minimize friction by escalating validation to higher levels only when there are indicators of potential fraud.

Alternative financial services vendors are improving their ability to verify identities, but they have to be able to respond continually to criminals' investments in their own technologies. This means these providers need to invest in more robust technology solutions that delve deeper into what the identity data means in order to better validate a customer's identity and stop fraud. Because fraudsters can readily purchase detailed consumer data on the dark Web, basic identity proofing or matching has become less relevant than new authentication algorithms or access to collaborative networks to deter fraud.

## Balancing Added Security against Customer Friction

Biometrics involving fingerprint and voice or facial recognition can provide additional layers of identification, but some executives question the added customer friction involved and note that these methods aren't generally available, or at best are awkward, during the account acquisition process. In many cases, biometric authentication during the account opening process for new customers isn't possible because the organization does not have a verified biometric credential to compare against. Even in customer use cases when biometrics are feasible, the extra friction required to capture the biometric might not be worthwhile. Mobile payment that requires thumbprint verification is easy because the customer holds the mobile device while tapping it to pay, but having to pause to take and transmit a photograph of oneself may make the process more trouble than it is worth to all but the most habitual "selfie" takers. Therefore, organizations need to balance the merits of security and verification methods versus unwanted friction and choose security tools that integrate with the account opening or payment process without pushing away legitimate customers.

[1] An identity obtained from gathering enough information on an individual to qualify to open or access an account.

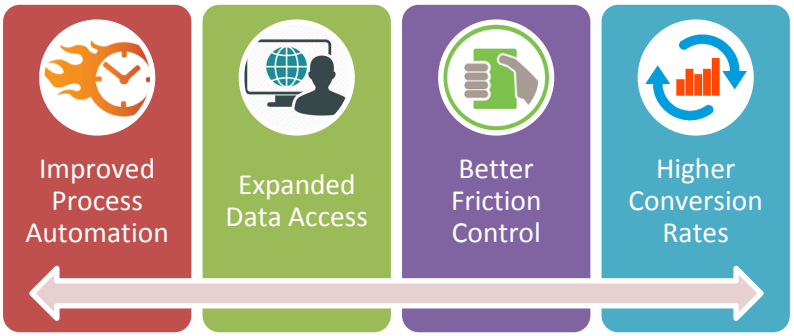


**Figure 1: Merits and Benefits of Improved Customer Authentication Processes**

Providers do not want prospective customers to feel too burdened with the security processes they have in place and turn to a competitor that doesn't require performing extra steps in the process. One Director of Fraud and Risk Management stated, "We don't have a lot of customer friction now, but we don't want to introduce any in future software iterations. If opening an account with our company gets too cumbersome, we'll lose business to our competitors." Concern regarding friction is well-founded, as evidenced by data from Mercator Advisory Group's 2014 CustomerMonitor Survey Series, which found that only one-third of U.S. consumers used even a password to protect access to their smartphone, much less any biometrics.

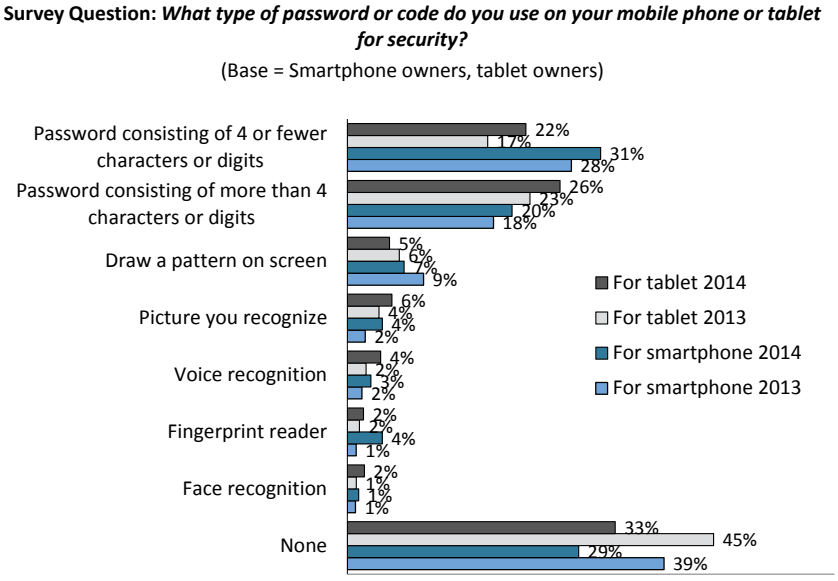


**Figure 2: Mercator Advisory Group CustomerMonitor Survey Series, Payments, 2013, 2014, Question 22**

Consumers themselves are increasingly security conscious today and more accustomed to participating in various levels of verification checks. Nevertheless, for providers that operate in a virtual environment, the consumer experience is all-important since it is so easy for prospective customers to abandon one process in favor of another. Leading alternative service providers understand this, which is why they maintain tight control over the due diligence process but also require a more sophisticated platform for risk management—one that incorporates KBA questions, ID validation, adaptive risk scoring, and curated fraud databases in a more seamless process as a means of managing risk and reducing post-account-acquisition losses.

Consumers might also turn away from companies perceived as less secure overall. Heightened security to defend against data breaches was highlighted by a Chief Information Officer who commented, "We haven't had any data breaches at our company, but we wouldn't have a pulse if we didn't focus on preventing data breaches or a robust defensive position. From our intelligence, the hackers aren't going away."

## New Financial Services Require New Fraud Prevention Strategies

Online and mobile-enabled financial services have opened entirely new segments to the market and widened the competitive environment for mainstream services like lending and depository accounts. Yet with these new channels come new risk management problems for participants to solve. The platforms that AFS providers have built enable them to transact with customers at a rapid pace, but it is that same alacrity that can lead to outsized fraud losses if criminals find and exploit a vulnerability in those platforms. Speed cuts both ways. The results of our study have demonstrated that AFS providers understand this and view authenticating the end user as a top investment priority. Executives we spoke to cite the importance of ensuring that before their companies give a consumer access, they know the individual and their credentials are one and the same. And given the incidence and depth of information of breaches taking place across the world, simplistic ID validation techniques or those that rely on self-reported information are no longer efficacious.

> *"We are always investing….It's an ongoing problem and the fraud is never static"* –Chief Information Officer

In this still-emerging market segment, stakeholders are most frequently competing in Web and mobile environments where face-to-face interactions are nonexistent. This is why we found that companies in the alternative financial services market were paying the most attention to the customer experience and increasingly fruitful data breaches as well as social engineering fraud strategies. Defending against these sophisticated data theft schemes requires equally sophisticated identity verification solutions that are capable of offering innovative and flexible platforms to address the risk inherent in these new markets.

Fraud is just as dynamic as new technologies. Fraudsters are gaining access to more data than ever before and constantly evolving their methods of attack on increasingly diverse targets. In such a rapidly evolving environment, there is an increasing amount of data and information to use in developing risk management strategies. Creating the optimal fraud detection environment requires incorporating known best practices gathered from other market participants and rationalized in an on-demand platform. We see strategies built in part from collaborative experiences and results as the most effective means of combating fraud and improving the overall user experience. State-of-the-art risk management platforms are now capable of enabling real-time decision-making using sophisticated algorithms and flexible architectures that balance these two dynamics in a way not possible from legacy post-transaction solutions or near-real-time solutions.

Onboarding is often considered the area of customer engagement with the greatest risk. Since ineffective risk management during account opening can result in significant fraud losses for providers and merchants, financial service providers increasingly utilize multiple layers of authentication and step-up authentication processes with ever-more sophisticated analysis of customer information based on device profile, history of transactions, geolocation, and log-in behavior to identify suspicious activities in the context of specific access requests. In this way, the account opening process can function not only to onboard new customers but also to establish a trusted and persistent identity credential that can follow the customer for the duration of the relationship with the financial services provider.

Traditionally, fraud and risk management has been a function of many different applications, some working in concert and some acting on specific transactions or consumer actions. This study finds that the alternative financial services market is in need of a comprehensive authentication environment, one that leverages a platform capable of seamless communication with account acquisition applications and able to access to IDV-specific real-time data not only on the applicant but also on the fraudster. This kind of new security environment can reduce friction, improve throughput, and streamline the entire account application process—all critical aspects of providing a competitive solution in this rapidly evolving new market of financial services.

## 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/