THE REBIRTH OF IDENTITY PROTECTION IN FINANCIAL SERVICES

May 2018

Sponsored by: EZShield

Independently produced by: JAVELIN
TABLE OF CONTENTS

Overview .................................................................................................................................................. 3
Executive Summary ............................................................................................................................... 4
Key Findings .......................................................................................................................................... 4
Recommendations ................................................................................................................................ 4
The Rise and Fall of Identity Protection in Banking ............................................................................. 6
Credit Monitoring Is Not Identity Protection ....................................................................................... 10
Consumers’ Need for an Identity Steward .............................................................................................. 12
Bringing Identity Protection Back to Banking ....................................................................................... 14
Endnotes ............................................................................................................................................... 15
Methodology ......................................................................................................................................... 15

TABLE OF FIGURES

Figure 1: Perceived Responsibility for Fraud Protection ........................................................................ 6
Figure 2: Change in Trust of Primary FI Among NAF Victims, by FI Where Fraudulent Accounts Were Opened ........................................................................................................................................ 7
Figure 3: Bureau’s Penalties Against IDPS Providers ........................................................................... 8
Figure 4: Volume of IDPS Subscriptions Offered Through Financial Institutions (2012–2017) ......................................................................................................................................................... 9
Figure 5: Aggregated Reasons for Monitoring Credit Report or Score, by Age .................................... 11
Figure 6: Concern About Fraud Among All Consumers and Fraud Victims (2013–2017) ............ 12
FOREWORD

This original report, sponsored by EZShield, examines the opportunity for financial institutions to offer identity protection services to their accountholders, in light of the fraud threats faced by digital-first consumers. With consumers facing a growing array of fraud threats, they are desperately in need of stewards that will help safeguard their identity and look to their financial institutions for help.

This research report was independently produced by Javelin Strategy & Research. Javelin Strategy & Research maintains complete independence in its data collection, findings, and analysis.

OVERVIEW

In 2012, regulators began to censure financial institutions and credit card issuers for certain practices related to identity protection offerings. After more than $2 billion in fines and settlements, the expectations of consumers and the institutions that seek to offer identity protection services (IDPS) have changed. In the interim, free credit scores have become a pervasive offering among major institutions.

Unfortunately, this has muddied the waters at a critical juncture when consumers are increasingly looking to their financial institutions to help protect their identities. A return to identity protection in banking would benefit consumers and FIs alike, but the road to adoption is complicated by mixed messages and bad memories.
EXECUTIVE SUMMARY

Key Findings
Consumers and FIs gain from a resurgence of IDPS in financial services. Consumers gain a valuable partner in protecting their identity, along with features that fill the gaps that even the most fraud-conscious consumers cannot address on their own. Financial institutions gain the opportunity to deepen relationships with customers and, by expanding the reach of their anti-fraud safeguards, further protect themselves from fraud risk.

Concern about fraud has reached a record high. Spikes in fraud and extensive media coverage around major breaches have caused consumers to become skeptical of the steps taken to protect their identities as the companies that store their data are repeatedly shown to be vulnerable. The proportion of consumers reporting that they are “very” or “extremely” concerned about fraud rose from 51% in 2016 to 69% in 2017.

Consumers see the need for an identity steward — and look to their FI. Although consumers tend to identify themselves as the most responsible party for protecting their accounts from fraud, the burden they place on their financial institution goes far beyond the responsibility they assign to other entities. Just less than two-thirds of consumers (61%) said that their financial institution(s) are among the two most responsible parties for protecting their accounts from fraud, compared to 37% for other companies storing the consumers’ data.

Securing accounts held at one institution isn’t enough. Victims who had fraudulent new accounts opened at an FI where they currently have accounts tended to gain trust in their FI, while victims where the accounts were opened at an FI where they do not currently have a relationship were much more likely to lose trust in their primary FI.

Credit monitoring alone isn’t identity protection. Though many consumers look to free credit monitoring services for fraud protection, alone these services leave dangerous gaps. Only a tenth of fraud victims had a fraudulent credit account opened in their name. Overemphasizing credit monitoring can actually run contrary to other anti-fraud best practices, such as establishing security freezes on credit reports when consumers do not need to open new accounts.

Recommendations
Offer a broad feature set to cover the risks faced by accountholders. Light identity protection offerings that focus on credit monitoring and resolution offer few opportunities for engagement and leave dangerous blind spots. As consumers increasingly see the security of their identity tied to the security of their data, providing tools to help secure users’ everyday activities can make an IDPS subscription relevant, even when fraud does not occur.

Educate customers about their fraud risks and the features that protect them. Any identity protection service that charges users must compete against an ever-widening array of free credit-monitoring tools. Although these tools are certainly useful for young consumers who are looking to build their financial lives, they should not be mistaken for anti-fraud tools. A broad set of features needs to be accompanied by an education campaign to demonstrate to non-users how those features...
can simplify their lives and secure their identities against fraud. Similarly, users should be regularly engaged so they can take the most advantage of the service and renew interest in underused services.

**Prioritize compliance in any potential partnerships.** Though the Consumer Financial Protection Bureau (CFPB) and other regulatory agencies have been silent for the past few years, the fines and penalties of 2012 to 2015 demonstrate the significant financial consequences of unethical practices, in addition to the damage to customer relationships. Transparency and prioritizing the needs of accountholders, rather than maximizing payout, can help further bolster accountholders’ perception that their FI is looking out for their best interests and is a reliable partner in protecting their identity.
The Rise and Fall of Identity Protection in Banking

Protection of accountholders' funds can be viewed as the fundamental promise of banking. Although the threats to those funds have evolved from highway robbers stopping stagecoaches to a much more sophisticated array of tactics, consumers' perceptions have not changed. Consumers naturally look to their financial institution as a key agent in protecting their identity from fraud.

Though consumers tend to identify themselves as the most responsible party for protecting their accounts from fraud, the burden they place on their financial institution goes far beyond the responsibility they assign to other entities. Nearly two-thirds of consumers (61%) said that their financial institution(s) are among the two most responsible parties for protecting their accounts from fraud, compared to 37% for other companies storing the consumers’ data (Figure 1).

Consumers See Themselves and Their FI as Partners in Fighting Fraud

Figure 1: Perceived Responsibility for Fraud Protection

Source: Javelin Strategy & Research, 2018
However, though financial institutions can provide the tools necessary to protect existing accounts from fraud — or at least to assist consumers when fraud does occur — they are limited in their ability to provide broader protection against fraud that occurs outside their walls. Unfortunately, fraud that occurs at other financial institutions can still have a deleterious impact on victims’ perceptions of their own financial institution. In fact, victims that had fraudulent new accounts opened at an FI where they currently have accounts tended to gain trust in their FI, while victims where the accounts were opened at an FI where they do not currently have a relationship were much more likely to lose trust.

This is probably because when accounts are opened at FIs where no relationship currently exists, the resolution process is much more challenging with no established customer history to fall back on to support the claims that the accounts are fraudulent. Additionally, the victim’s actual financial institution is unlikely to be involved in the resolution process, giving them no opportunities to directly shore up their reputation against spillover effects.

Partnerships with other organizations, such as IDPS providers, have helped to broaden FIs’ anti-fraud measures for accounts at other institutions. With the intuitive connection between fraud protection and financial services, these partnerships could flourish. In 2017, subscriptions obtained through a financial institution remained the second-most popular source for identity protection services — next to going directly to a provider — with about 23 million active subscriptions.1

---

Even Fraud at Other Institutions Can Erode Confidence in an FI

Figure 2: Change in Trust of Primary FI Among NAF Victims, by FI Where Fraudulent Accounts Were Opened

<table>
<thead>
<tr>
<th></th>
<th>Increased trust</th>
<th>No change</th>
<th>Decreased trust</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fraudulent new accounts at current FI</td>
<td>62%</td>
<td>21%</td>
<td>17%</td>
</tr>
<tr>
<td>Fraudulent new accounts at another FI</td>
<td>25%</td>
<td>28%</td>
<td>47%</td>
</tr>
</tbody>
</table>

Source: Javelin Strategy & Research, 2018
However, for several years, these partnerships came under heavy scrutiny. Beginning in 2012, the CFPB and other regulatory agencies began targeting unethical sales and business practices at financial institutions that offered identity protection and credit monitoring services. These regulatory actions were not prompted directly by failures of the identity protection services but by a number of deceptive or otherwise unethical sales and marketing practices, including:

- Failure to fully enroll users before charging the full fee. This resulted in millions of users failing to complete secondary activation steps and consequently going without access to credit monitoring services, despite being charged as if the full services were active.
- Misleading consumers about the benefits of features included within the services.

- Aggressive sales practices that used leading questions to receive billing approval from customers or that construed an ambiguous response as an approval.

From July 2012 to July 2015, the CFPB and other regulatory agencies assessed a total of $173 million in civil penalties and an estimated $2.2 billion in consumer refunds, for a total of about $2.4 billion. However, since July 2015, the CFPB has been silent on the issue (Figure 3).

With the regulatory penalties came an attendant decline in the prevalence of identity protection services offered through financial institutions. In 2012, 38% of all identity protection subscriptions were obtained through the subscriber’s financial institution, totaling 59.5 million subscriptions. In 2017, that figure...
had fallen to 22% of subscriptions, or a total of 22.7 million (Figure 4).

The good news for financial institutions and identity protection service providers alike is that the regulatory action against these FIs and providers were not due to any inherent flaw in identity protection services per se, but only in the targeted unethical practices in which they were delivered. This opens the door for conscientious partnerships that are mindful of sales and marketing practices to continue delivering value to consumers.

With the evolution of fraud in the past several years, the consumer need for partners in protecting their identity has perhaps never been greater. Many factors have converged to drive fraudsters to fraud types that are not only more difficult for consumers to detect on their own but that also have a much more significant effect on consumers and their relationship with their FIs. Effectively meeting these needs means delivering broader services to accountholders that redefine the purpose of identity protection.

**Identity Protection Through FIs Has Not Rebounded After Regulatory Penalties**

*2016 data estimated from 2015 and 2017 data points*

Source: Javelin Strategy & Research, 2018
CREDIT MONITORING IS NOT IDENTITY PROTECTION

As consumers seek out partners to help secure their identities, financial institutions and identity protection service providers must shout over the din caused by a proliferation of free options to monitor their credit activity. Services like Credit Karma and Credit Sesame are well known and are especially popular among young consumers. About a quarter of the top 30 financial institutions in the U.S. offer accountholders the ability to track their credit scores through online or mobile banking. Some, such as Discover, have even broadened the offerings to be free to all consumers, regardless of whether they have an account with the institution.

“How is it being marketed? We have positioned it as a financial education tool to clear up confusion around what constitutes a good credit score. Identifying fraud has not been a piece of that (messaging).”

Product Strategy Executive
Large U.S. Credit Union

in that users of credit-monitoring tools do have more opportunities to identify fraudulently opened credit accounts than consumers who do not regularly check their credit report. However, treating these tools as a replacement for full-featured identity protection tools leaves consumers with dangerous blind spots.

This view is especially prevalent among older consumers, many of whom already have established finances and have less need to open new accounts regularly. Among consumers 65 and older, 40% monitor their credit report solely to detect fraud, and for an additional 32%, fraud protection is one of the primary reasons they monitor their credit report (Figure 5).

Although monitoring for credit-related accounts opened in consumers’ names is a crucial element of rapidly detecting fraud, relying on credit-monitoring services alone has several flaws.

For users of these types of services, it is tempting to view them as a fraud protection tool as well. There is some merit to the idea — which is part of what makes it so tempting —

Typically aimed at building financial health, these offerings frequently include credit score trackers, as well as an enumeration of the information contained on a subscriber’s credit report, with indicators of what is positively or negatively contributing to his credit score.

For users of these types of services, it is tempting to view them as a fraud protection tool as well. There is some merit to the idea — which is part of what makes it so tempting —

“The thing is that Credit Karma makes it hard for us to sell these services to customers. Almost every bank I know of is offering them for free. I think it is table stakes to be in the game right now.”

Consumer Credit Executive
Regional U.S. Financial Institution

First, this protection is capable of detecting only a small proportion of fraud schemes. Fewer than 10% of fraud victims have a new credit-oriented account opened in their name. The most prevalent fraud types — existing card
Older Consumers Monitor Their Credit Principally to Combat Fraud

Figure 5: Aggregated Reasons for Monitoring Credit Report or Score, by Age

Source: Javelin Strategy & Research, 2018

Fraud and existing non-card fraud — will only appear obliquely on a credit report. A large purchase on an existing credit card account will manifest as a balance change on the account the next time it is reported to the credit bureau. However, neither the bureaus nor the identity protection provider has the capability of differentiating between a balance change due to a legitimate purchase and a fraudulent transaction.

Second, overemphasizing credit monitoring can lead to a false sense of security. For consumers who have established financial histories, freezing credit reports can provide a more effective safeguard against fraud with minimal imposition on the rest of their lives.

Freezing credit reports is simply impractical for some because they need to open new accounts. However, consumers and the organizations that protect them should also keep in mind that credit-oriented safeguards will not stop other forms of identity theft, such as tax fraud and medical identity theft.

“We do not explicitly say that it is not for fraud monitoring... Now if they see their score decline over a short period of time, we have educational resources that encourage them to get in contact with the right parties around fraud. But we really want you to understand credit.”

Product Strategy Executive Large U.S. Credit Union
CONSUMERS’ NEED FOR AN IDENTITY STEWARD

The consumer need for identity protection partnerships has never been greater. Fraud of all types reached record heights in 2017. The most significant spikes were observed in fraud types that are most damaging to consumers, as well as the most challenging for consumers to prevent and detect without help.

Spikes in fraud and extensive media coverage about major breaches have caused consumers to become skeptical of the steps taken to protect their identities as the companies that store their data are repeatedly shown to be vulnerable. The proportion of consumers reporting that they are “very” or “extremely” concerned about fraud rose from 51% in 2016 to 69% in 2017 (Figure 6).

Failure to build broader identity protection partnerships causes FIs to miss an opportunity to build stronger relationships with their accountholders by providing them the tools they need to fill in the gaps in their own anti-fraud efforts. Several key features and capabilities can supplement the fraud protections that financial institutions offer:

“We do make credit monitoring available through one of the bureaus to our members for a fee. I remember there was a lot of interest in it after the Equifax breach. So we were more front and center about it afterwards.”

Product Strategy Executive
Large U.S. Credit Union

Consumers’ Concerns About Fraud Spike in 2017

Figure 6: Concern About Fraud Among All Consumers and Fraud Victims (2013-2017)

Source: Javelin Strategy & Research, 2018
• **Broad new-account detection:** New-account fraud at institutions where consumers do not have a current relationship can be nearly impossible for consumers to detect alone until the fraud is complete and the account goes into collections. But this is where tools like credit monitoring and other account-opening monitoring tools provided by identity protection providers work particularly well.

• **Account aggregation capabilities:** Being able to monitor all financial accounts in a single portal can supplement account monitoring by a subscriber’s primary financial institution and offer protection for inactive or low-use accounts that a subscriber might not regularly monitor but which are still targets for fraudsters.

• **PII exposure monitoring:** Tools that notify consumers of recent breaches and monitor for sale of customers’ personally identifiable information (PII) on criminal marketplaces can provide a buffer against account takeover, which is the single most prominent reason that fraud victims switch banks.

• **Data protection features:** Partnerships with data protection providers, such as password managers or anti-malware services, can more broadly supplement financial institutions' anti-fraud efforts by reducing their accountholders’ exposure. Potential risks to accountholders are often caused by lax security on third-party sites. Fraudsters have proven themselves adept at using side channels to compromise financial accounts. Some take over accounts at retail sites to accomplish card-not-present fraud, and others take advantage of reused credentials after a breach at an apparently unrelated site to gain access into their victims’ financial accounts.
BRINGING IDENTITY PROTECTION BACK TO BANKING

Both consumers and financial institutions stand to gain from a resurgence in identity protection services offered through financial institutions. Consumers gain a valuable partner in protecting their identity, along with features that fill the gaps that even the most fraud-conscious consumers cannot address on their own. Financial institutions gain the opportunity to deepen relationships with customers and, by expanding the reach of their anti-fraud safeguards, protect themselves from fraud risk.

To successfully roll out identity protection for their customers, any identity protection service offered through a financial institution should consist of a broad feature set to span the risks faced by accountholders. Light identity protection offerings that focus on credit monitoring and resolution offer few opportunities for engagement, and they leave dangerous blind spots. As consumers increasingly see the security of their identity tied to the security of their data, providing tools to help secure users’ everyday activities can make an IDPS subscription relevant, even when fraud does not occur.

Any identity protection service that charges users must compete against an ever-widening array of free credit-monitoring tools. Although these tools are certainly useful for young consumers who are looking to build their financial lives, they should not be mistaken for anti-fraud tools. A broad set of features needs to be accompanied by an education campaign to demonstrate to non-users how those features can simplify their lives and secure their identity against fraud. Similarly, users should be regularly engaged so that they can take full advantage of the service and renew interest in underused services.

Compliance should be prioritized in any potential partnerships. While the CFPB and other regulatory agencies have been silent for the past few years, the fines and penalties of 2012 to 2015 demonstrate the significant financial consequences to unethical practices, in addition to the damage to customer relationships. Transparency and prioritizing the needs of accountholders — rather than maximizing payout — can help bolster accountholders’ perceptions that their FI is a reliable partner in protecting their identities, and ultimately looking out for their best interests.
METHODOLOGY

Consumer data in this report is based on information gathered in several Javelin surveys administered in 2014, 2015, 2016, and 2017. Data was gathered and weighted to reflect a representative sample of the adult U.S. population:

- A random-sample panel of 2,129 respondents in a December 2017 online survey. The margin of sampling error is ±2.12 percentage points at the 95% confidence level. The margin of sampling error is higher for questions answered by subsegments.
- A random-sample panel of 5,000 respondents in an October/November 2017 online survey. The margin of sampling error is ±1.39 percentage points at the 95% confidence level. The margin of sampling error is higher for questions answered by subsegments.
- A random-sample panel of 5,028 respondents in a November 2016 online survey. The margin of sampling error is ±1.40 percentage points at the 95% confidence level. The margin of sampling error is higher for questions answered by subsegments.
- A random-sample panel of 3,100 respondents in an August/September 2015 online survey. The margin of sampling error is ±1.76 percentage points at the 95% confidence level. The margin of sampling error is higher for questions answered by subsegments.
- A random sample panel of 3,100 respondents in an August/September 2014 online survey, the margin of sampling error is ±1.76 percentage points at the 95% confidence level. The margin of sampling error is higher for questions answered by subsegments.

ENDNOTES

ABOUT JAVELIN STRATEGY & RESEARCH

Javelin Strategy & Research, a Greenwich Associates LLC company, is a research-based consulting firm that advises its clients to make smarter business decisions in a digital financial world. Our analysts offer unbiased, actionable insights and unearth opportunities that help financial institutions, government entities, payment companies, merchants, and other technology providers.

Authors:  
Al Pascual, SVP Research and Head of Fraud & Security  
Kyle Marchini, Senior Analyst, Fraud Management

Contributors:  
James Wilson, Analyst, Digital Lending

Editor:  
Chuck Ervin

Publication Date:  
May 2018

ABOUT EZSHIELD

EZShield helps financial institutions and other trusted partners protect their most valuable asset — their customer relationships — through secure, digital identity protection and resolution services that enhance the value of existing products. The company is consistently recognized by Javelin as a leader in Identity Protection. Owned by the Wicks Group of Companies, L.L.C., EZShield supports thousands of financial institutions through its award-winning solutions, delivered on a secure, flexible platform that is backed by best-in-class customer support.

www.ezshield.com

© 2018 GA Javelin LLC (dba as “Javelin Strategy & Research”) is a Greenwich Associates LLC company. All rights reserved. No portion of these materials may be copied, reproduced, distributed or transmitted, electronically or otherwise, to external parties or publicly without the written permission of Javelin Strategy & Research. GA Javelin may also have rights in certain other marks used in these materials.