The 2017 Field Guide to Identity Crime

The Financial Institution’s Guide to Protecting Account Holders
Don’t lose account holders to identity crimes.

In 2016, there were 35.2 million identity crime victims in the U.S.¹

That’s a new victim every second.

Identity crimes can rob your financial institution of account holder loyalty, especially if you’re

Your account holders come to you for financial expertise, and they expect you to bring them certain levels of protection.

They trust you to secure their finances and to be a resource in the event of identity crime. This means that identity protection should be part of your service offering.

Protecting your account holders’ identities is now part of delivering on expectations and growing brand loyalty.

It’s time to evaluate your post-fraud protocols to better understand the account holder experience in this new age of identity security.

This e-book was created to empower financial institutions with information needed to understand the current state of identity crimes and offer comprehensive protection solutions.

¹ Javelin Strategy & Research,
Fighting Back Against Identity Thieves

UNDERSTANDING IDENTITY CRIMES ........................................ 4

THE FLIGHT-POST-FRAUD PHENOMENON ...................... 8

IDENTITY THEFT ..................................................................... 11

OUR CUSTOMER SERVICE TEAM ....................................... 15

IT STARTS WITH YOU ............................................................. 16

ONGOING EDUCATION .......................................................... 18

TAKE THE NEXT STEP ........................................................... 19
35.2 Million

Americans were victims of identity crimes in 2016.¹

¹ Javelin Strategy & Research 2017
Today’s “identity crimes” come in all shapes and sizes and continue to evolve daily. Such crimes can be broken down into the following three categories:

- Lost/Stolen Personally Identifiable Information (PII)
- Payments Fraud
- Identity Theft

When a criminal assumes a false identity, it impacts every facet of the victim’s life. Criminals can manipulate financial, medical, government, criminal and even employment records. This wide breadth of misuse makes identity crimes hard to detect, and even harder to repair without the right resources.

FAST FACT:
One in five people have used 123456 to “protect” their accounts, yikes! (The most common password of 2016)

-KeeperSecurity, 2017
Think you know everything about identity crimes? Think again.

FAST FACT:
A credit freeze will not stop identity theft! It only requires extra verification to open new accounts in your name; it will not close accounts a criminal has already opened in your name.

*Javelin 2016 Identity Fraud Report  | **Identity Theft Resource Center, 2017

---

**Lost/Stolen PII**
Social Security number, date of birth, credit card information, etc.
1 in 5 data breach victims suffered fraud in 2015*
36 million sensitive records were exposed in data breaches in 2016**

**Payments Fraud**
The use of an existing financial vehicle (credit card, checking account number, bank account number) to steal funds
$16 billion lost annually*

**Identity Theft**
Use of lost/stolen PII to open new accounts in the victim’s name.
$2.3 billion annual losses*
18 hours spent fighting a single event*
Your Good Name Has a Price.

Your account holders’ PII is valuable — and identity thieves have several tactics for getting their hands on it.

- Dumpster diving
- Phishing
- Lost phone
- Online shopping
- Stolen wallet
- Data breach
- Mail theft
- Change of address
- Credit card skimming

Once information is snatched, it often makes its way onto the dark web. The dark web allows for anonymous web surfing, which creates a breeding ground for criminal activity and black market websites. These sites act like any other online retailer to facilitate the illegal sale of PII.

---

### Black Market Value of PII*

<table>
<thead>
<tr>
<th>Type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Visa or Date of Birth</td>
<td>$7</td>
</tr>
<tr>
<td>Medical</td>
<td>$11</td>
</tr>
<tr>
<td>Popular Email Account</td>
<td>$20</td>
</tr>
<tr>
<td>Bank</td>
<td>$129</td>
</tr>
<tr>
<td>Complete</td>
<td>$300</td>
</tr>
</tbody>
</table>

* Dell SecureWorks 2014,
The Flight-Post-Fraud Phenomenon

Fraud is a primary catalyst for bank switching, especially when checking accounts are compromised. Accountholders will also stop using certain banking functions, to feel more in control of their finances post-fraud.

2017 Checking Account Post-Fraud Behavior*

Post-fraud financial behavior among all fraud victim, checking account, and credit card fraud victims

<table>
<thead>
<tr>
<th>Percentage of Fraud Victims</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switched Forms of Payment</td>
</tr>
<tr>
<td>Credit Card Fraud</td>
</tr>
<tr>
<td>Checking Account Fraud</td>
</tr>
<tr>
<td>All Fraud Victims</td>
</tr>
<tr>
<td>Stopped Banking Online</td>
</tr>
<tr>
<td>Credit Card Fraud</td>
</tr>
<tr>
<td>Checking Account Fraud</td>
</tr>
<tr>
<td>All Fraud Victims</td>
</tr>
</tbody>
</table>

*Javelin Strategy & Research
Nearly

1 million

account holders switched financial institutions post-fraud in 2016.*

Younger account holders are most at risk of switching post-fraud.

*Understanding Post-Fraud Bank Switch, Javelin Strategy & Research
Age Is a Major Determinant of Loyalty

Fraud events tied directly to your financial institution can often be resolved internally. However, identity crimes frequently involve personal information getting into the wrong hands, which leads to the potential for continued misuse. Without comprehensive resolution, the account holder is left with uncertainty that can ultimately erode loyalty.

FAST FACT:
One in five fraud victims who switched financial institutions post-fraud never alerted their bank or credit union to the incident.

-Javelin Strategy & Research, 2017
Will You Be Ready for Identity Theft?

Different accountholder groups face different identity crime risks.

Understanding their unique risks is key in developing successful, value-add offerings that will have a direct impact on loyalty. Be prepared to meet their unique post-fraud needs through an EZShield partnership. Our proactive approach covers the gamut of identity crimes to help:

### Boomers are the Most Victimized Demographic*

<table>
<thead>
<tr>
<th>Category</th>
<th>Millennials</th>
<th>Gen X</th>
<th>Baby Boomers</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Fraud</td>
<td>5.45%</td>
<td>5.81%</td>
<td>7.12%</td>
</tr>
<tr>
<td>Existing Card Fraud</td>
<td>4%</td>
<td>4.76%</td>
<td>6.07%</td>
</tr>
<tr>
<td>Existing Non-Card Fraud</td>
<td>1.14%</td>
<td>0.90%</td>
<td>1.56%</td>
</tr>
<tr>
<td>Account Takeover</td>
<td>0.61%</td>
<td>0.66%</td>
<td>0.55%</td>
</tr>
<tr>
<td>New Account Fraud</td>
<td>0.55%</td>
<td>0.77%</td>
<td>0.90%</td>
</tr>
</tbody>
</table>

*© 2017 GA Javelin LLC
Protect your bottom line by securing their identity.

Preventing account-related fraud can save millions for your financial institution, so it’s vital to mount effective — and broad-ranging — consumer protection efforts.

In late 2016, Javelin reported that one in ten defrauded account holders switched financial institutions post-fraud. They took $4 billion in credit card spending with them.

We provide the tools to keep their PII safe, including:

- Tailored education and fraud prevention tips
  - Monthly activity report
  - Breach alerts
- Secure online identity vault, digital wallet and password manager

EZShield helps you and your account holders stop fraudulent activity before it starts, saving time, money and frustration.

*ACI Worldwide and Aite Group, 2012*
Early detection of fraud or suspicious activity is crucial.

Fraudsters use many forums to obtain personal and confidential information. EZShield constantly monitors activity and provides regular detailed reports to your account holders, including:

- Credit Monitoring
- Internet Monitoring
- Public Records Monitoring
- Financial Transaction Monitoring

You want your account holders to feel comfortable using your financial institution’s products and services. We help you provide that peace of mind because we’re always watching. From publicly available information to the Internet’s black market, we’re on the lookout for red flags.
Putting consumers back in control

We call it End2End Defense™ – a 32-step process that starts with a dedicated resolution specialist to walk the victim through the entire process. A few of these critical steps include:

- Updating online passwords
- Replacing checks
- Replacing debit card
- Opening new accounts as necessary
- Long-term monitoring in the event of fraud

A partnership with EZShield puts account holders back in control of their good name, right when they need it most.
Our Customer Service Team

When fraud happens, our team of resolution experts walks victims through the process to get their life back on track and help prevent the issue from happening again.

- **Always available**
  - 24/7/365 customer support
  - U.S.-based representatives
  - Multilingual Spanish and French support

- **Single point of contact**
  - Victims aren’t passed around
  - Dedicated resolution specialist for each case

- **Expert assistance**
  - Industry memberships and certifications maintained annually
  - Average tenure for senior specialist: 7 years

- **Continuous follow-up**
  - Specialists have a servicing profile, not selling
  - Fully managed support
EZShield works directly with you to create an integrated communications program based on your goals, account holder needs and branded to your specifications. Here’s what your communication tool kit includes:

- Email
- 24/7 phone support
- Social media
- Dedicated website
- Mobile application
- Marketing collateral

Communication is Key

EZShield’s integrated communication program and user-friendly resources have won 18 Communicator Awards from the Academy of Interactive and Visual Arts.

FAST FACT:
The average American has 150 online accounts. (That’s a lot of passwords to remember)

- DashLane, 2017
Identity Protection Takes a Personal Approach

Breaking down consumer personas to find your perfect communication strategy.

FAST FACT:
Students take 3x longer to detect fraud
-Javelin Strategy & Research, 2017

Offline Consumer
• Prefers in-branch visits to online banking
• Reach with-branch marketing materials and live support

Social Networker
• Young and tech-savvy
• Reach with multiple social media platforms and a dedicated website

E-Commerce Shopper
• High monthly transactions; highest risk of fraud
• Reach via targeted email marketing campaigns

Connected Consumer
• Early adopter of new technology
• Reach with a user-friendly mobile application
Ongoing Education

Fraudsters are always seeking new opportunities to steal personal and financial information. That’s why EZShield created fightingidentitycrimes.com – a central location for the latest information on:

- Personal protection
- Small business protection
- Breach and scam news
- Identity protection resources

Providing the right tools and resources goes a long way to empowering account holders and enhancing their loyalty to your financial institution.
Take the Next Step

If you are interested in finding out more about how to protect your account holders while meeting your goals to drive fee income, acquire account holders and grow loyalty, please contact us to schedule a demo. Find out why EZShield could be the ideal identity protection partner for your financial institution.

Schedule a Demo
https://www.ezshield.com/schedule-a-demo/

Check out our suite of products online
https://www.ezshield.com/consumer-

Give us a call at 1.877.339.0027

Sign up for the EZShield newsletter
https://www.ezshield.com/partner-newsletter-signup/