Don’t lose account holders to identity crimes.

Identity crimes can rob your financial institution of account holder loyalty, especially if you’re not prepared.

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

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

Your account holders now expect you to protect their identities, which drives loyalty and top-of-mind awareness to your institution.

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

This e-book was created to empower financial institutions with the information you need to understand the current state of identity crimes and to offer comprehensive protection solutions.
Fight Back Against Identity Thieves

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

CONSUMER BEHAVIOR POST-FRAUD ............................... 8

A PARTNER IN FIGHTING FRAUD .................................... 10

COMPREHENSIVE IDENTITY SOLUTIONS .............................. 14

OUR CUSTOMER SERVICE TEAM ..................................... 18

COMMUNICATION IS KEY .................................................. 19

TAKE THE NEXT STEP ................................................... 22
Total Number of Identity Crime Victims at Record High

- **79.1 million** Americans were victims of identity crimes in 2017
- **2 new** identity crime victims every second
- **$16.8 billion stolen** by fraudsters from U.S. consumers

Identity Fraud Study, Javelin Strategy & Research, 2018
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 or Stolen Personally Identifiable Information (PII)**
- **Payments Fraud**
- **Identity Theft**

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

**FAST FACT**

Nearly 3 percent of people have used 123456 to “protect” their accounts! (The worst password of 2017)
Think you know everything about identity crimes? Think again.

**FAST FACT**
A credit freeze will not stop identity theft! It will only make extra verification necessary to open new accounts in your name, and it will not close accounts a criminal has already opened in your name.

- **Lost/Stolen PII**
  Social Security number, date of birth, address, credit card information, etc.
  - 1 in 3 data breach victims suffered fraud in 2016*
  - 4.5 billion data records were compromised worldwide in the first half of 2018**

- **Payments Fraud**
  The use of an existing financial vehicle (credit card, checking account number, bank account number) to steal funds.
  - Victims pay an average of $238 for existing non-card fraud*

- **Identity Theft**
  The use of lost or stolen PII to takeover a victim’s account.
  - $5.1 billion annual losses*
  - 16 hours spent fighting a single event*

*Identity Fraud Study, Javelin Strategy & Research, 2018 | **Gemalto Breach Level Index
What’s an identity worth on the Dark Web?

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 obtained, it often makes its way onto the dark web where people can conduct business anonymously. This creates a breeding ground for criminal activity and black market websites that act like any other online retailer — except they illegally sell personally identifiable information.

### Black Market Value of PII*

<table>
<thead>
<tr>
<th>PII Type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credit Card</td>
<td>$7</td>
</tr>
<tr>
<td>Date of Birth</td>
<td>$11</td>
</tr>
<tr>
<td>Medical Insurance</td>
<td>$20</td>
</tr>
<tr>
<td>Email Account</td>
<td>$129</td>
</tr>
<tr>
<td>Bank Account</td>
<td>$300</td>
</tr>
<tr>
<td>Complete Identity</td>
<td>$1,200</td>
</tr>
</tbody>
</table>

* Dell SecureWorks 2016 & 2017
Nearly 1 million account holders switched financial institutions post-fraud in 2015.*

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

*Understanding Post-Fraud Bank Switching, Javelin Strategy & Research, 2016
Fraudulent activity 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 a comprehensive resolution, the account holder is left with uncertainty that can erode their loyalty.

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

Switched Forms of Payment
- Checking account fraud victims: 22%
- Credit card fraud victims: 13%
- All fraud victims: 16%

Switched Primary Financial Institution
- Checking account fraud victims: 13%
- Credit card fraud victims: 4%
- All fraud victims: 5%

Understanding Post-Fraud Bank Switching, Javelin Strategy & Research, 2016

Javelin Strategy & Research, 2018
Protection of account holders’ funds can be viewed as the fundamental promise of banking. As such, 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, the burden they place on their financial institution goes far beyond the responsibility they assign to other entities.

Consumers See Themselves and Their FI as Partners in Fighting Fraud

<table>
<thead>
<tr>
<th>Source of Responsibility</th>
<th>Percentage of Consumers</th>
</tr>
</thead>
<tbody>
<tr>
<td>My Bank</td>
<td>25% Most responsibility</td>
</tr>
<tr>
<td>Myself</td>
<td>42% Most responsibility</td>
</tr>
<tr>
<td>Companies and institutions storing my data</td>
<td>17% Most responsibility</td>
</tr>
<tr>
<td>Merchants</td>
<td>4%</td>
</tr>
<tr>
<td>Identity protection service providers</td>
<td>5% Most responsibility</td>
</tr>
<tr>
<td>The government</td>
<td>5%</td>
</tr>
<tr>
<td>Law enforcement</td>
<td>4%</td>
</tr>
</tbody>
</table>

Javelin Strategy & Research, 2018
Although financial institutions provide the tools necessary to protect their existing account holders from fraud, they are limited in their ability to provide broader protection against fraud that occurs outside their walls.

With that in mind, only securing the accounts at your institution is not enough. In fact, when fraud hits, consumers are more forgiving if it happened within the current Financial Institution (FI) they do business with. What's interesting is that if consumers have fraud occur outside of their primary FI, the distrust is transferred back to the primary FI.

**Change in trust of primary FI among New Account Fraud (NAF) victims, fraudulent accounts were opened:**

- **Opened at current FI:**
  - Increased trust: 17%
  - No change: 62%
  - Decreased trust: 21%

- **Opened at other FI:**
  - Increased trust: 25%
  - No change: 28%
  - Decreased trust: 47%

Javelin Strategy & Research, 2018
Consumers’ Need for an Identity Steward

Fraud of all types reached record heights in 2017. The proportion of consumers reporting they are “very” or “extremely” concerned about fraud rose from 51% in 2016 to 69% in 2017.

The consumer need for identity protection partnerships has never been greater. Be prepared to meet this growing need through an EZShield partnership. Our proactive approach covers the gamut of identity crimes to help fill the gaps in protection.

Consumers’ Concerns About Fraud Spike in 2017

- **2013**: 57% concerned
- **2014**: 67% concerned
- **2015**: 66% concerned
- **2016**: 69% concerned
- **2017**: 82% concerned

Javelin Strategy & Research, 2018
Adding Identity Protection into the mix offers a comprehensive solution for consumers that meets the needs of your Financial Institution.

There is a natural intersection for both cybersecurity and financial health and the common need is for account holders to have the tools they need to protect themselves.

- Identify vulnerabilities
- Manage third-party risks
- Monitor, Alert, Control, Recover
- Educate and Assist
- Amount of savings
- Loan worthiness
Monitor

Early detection of fraud or suspicious activity is crucial.

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

- Credit Monitoring
- Dark Web Monitoring
- Public Records Monitoring
- Financial Transaction Monitoring
- Account 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 ever on the lookout for red flags.
Alert

Discover faster and act sooner.

If any of your account holders’ vault-stored information is found on the dark web, our dark web monitoring will send them alerts via email (and push notifications with the EZShield mobile app) so they know when their information has been exposed. This includes:

- Name
- Street Address
- Driver’s License
- Social Security Number
- Email Addresses
- Medical ID Cards
- Passports

These alerts will help them know when they need to take extra precautions to secure their identity and thwart identity theft.

Tony received a cyber alert to his EZShield online account to notify him that his personal information may have been compromised.

“I never expected to be contacted by phone concerning potential threats. I figured I was on my own. I appreciate you guys watching out for me! Love your service and recommend you to everyone I can.” – Tony B. Case #56376
Control

Protect your bottom line by securing their identity.

Providing proactive monitoring for 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, taking $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 identity reports
  • Breach alerts
• Secure online identity vault, digital wallet and password manager

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

Jason received a letter in the mail from the Internal Revenue Service (IRS) indicating that he owed $1,900 in taxes for wages claimed in Texas.

“If I didn’t have this I wouldn’t know where to turn. It’s comforting knowing if fraud happens to me again, EZShield will take care of me.” – Jason C. Case #31758
Recover

Putting consumers back in control.

We call it EZShield Restoration, a 32-step process that starts with a dedicated Resolution Specialist to walk the victim through the procedure from start to finish. 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
- Disputing charges

Your partnership with us puts your account holders back in control of their good name, right when they need it most.

Identity crime consequences include:

- **30% of victims** sought financial assistance from family or friends
- **32% of victims** had problems at their place of employment
- **41% of victims** could not pay their bills
- **52% of victims** have yet to resolve the issue to their satisfaction a year later
- **68% of victims** feel a sense of powerlessness or helplessness

ITRC Identity Theft: The Aftermath 2018
When fraud happens, our team of understanding experts walk victims through the resolution process to get their life back on track and help protect against future threats.

IN-HOUSE, U.S. CALL CENTER
- If your identity is compromised, you’ll be speaking to a certified Resolution Specialist located in-house.
- Our team has an average tenure of 7 years.

DEDICATED RESOURCE
- We take your identity theft or fraud claim personally.
- That’s why you’ll be assigned a dedicated Resolution Specialist until your issue is resolved completely.

SECURITY MATTERS
- Our people, processes, and systems maintain ironclad security measures at all times.
- Your personal information is handled securely, using triple-layer data encryption.

HIGH-TOUCH
- When you work with one of our Resolution Specialists, you’ll never have to worry about where you stand.
- From first contact until completed restoration, it’s the satisfaction of our customers that matters most.

“Our customers receive the same high quality service from the Resolution Specialists as they receive from our Frandsen Bank employees.”

Karen Brekke, EVP Chief Administrative Officer, Frandsen Bank & Trust
Multi-Channel communications that deliver the right message at the right time.

**FAST FACT**

The average American has 150 online accounts (That's a lot of passwords to remember!)

DashLane, 2017

Our integrated communications program and user-friendly resources have won 18 Communicator Awards from the Academy of Interactive and Visual Arts since 2015.

We work directly with you to create an integrated communication program that’s based on your goals and branded to your specifications. Your communication tool kit includes:

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

“I would absolutely recommend EZShield. They were so willing to listen and talk about program options that were outside of the normal boundaries of the programs they already had. The company is very forward-thinking, flexible, innovative and strive[s] to create the best customer experience possible.”

Karen Brekke, EVP Chief Administrative Officer, Frandsen Bank & Trust
Identity Protection Takes a Personal Approach

Breaking down consumer personas to find your perfect communication strategy.

FAST FACT
Unlike adults who might actively monitor their credit reports and financial accounts, students take 3x longer to detect fraud.

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 dedicated website

E-Commerce Shopper
• High number of monthly transactions; at highest risk of fraud
• Reach via targeted email and online marketing campaign

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 we 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 toward empowering account holders and enhancing their loyalty to your financial institution.
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.
EZShield
A Sontiq™ Brand

Our Mobile App Recognized by
BankNews for Excellence in:
Authentication | Fraud Protection | Cybersecurity

Learn More

Mobile Defense Suite