THE 2019 FIELD GUIDE TO IDENTITY CRIME

The Financial Institution’s Guide to Protecting Account Holders in 2020
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 — whether transacting by mobile device, online, or in person.

They trust you to keep their finances secure and to be a resource in the event of an identity crime. This means that 24/7/365 identity protection should be part of your service offering.

Your account holders not only expect you to protect their identities, which drives loyalty and top-of-mind awareness to your Financial Institution (FI), but they also want a more personalized experience when they bank with you. And regulators expect you to maintain a secure and compliant digital perimeter in order to ward off mounting cybersecurity threats.

In a continuously evolving digital world, you are responsible for managing more data, across more devices — all while driving innovation and exceeding customer expectations.

It’s always the right 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.
PROTECT AGAINST
IDENTITY THIEVES

Identity Crime is Growing ............................ 4
Consumer Behavior Post-Fraud ..................... 9
A Partner in Fighting Fraud ............................ 11
Comprehensive Identity Solutions .................. 14
Award-Winning Customer Service .................. 19
Communications is Key ............................... 20
Take the Next Step .................................... 23
IDENTITY CRIME IS GROWING — AND PERVASIVE

TOTAL NUMBER OF IDENTITY VICTIMS CONTINUES TO GROW

• **160 million** sensitive records of Americans were exposed in the first 10 months of 2019

• **Financial sector** had the highest percentage of sensitive breaches in 2019 (61 percent)

• **$26 billion** stolen through business email and email account compromise (BEC/EAC) scams, June 2016–July 2019

• **Being a victim of identity theft** is a major concern for Americans (67 percent), and mobile users are the most worried about having their identity stolen (72 percent)

WAYS CUSTOMER DATA WAS EXPOSED BY BANKS IN 2019

<table>
<thead>
<tr>
<th>Way</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unauthorized access</td>
<td></td>
</tr>
<tr>
<td>Hacking/Intrusion</td>
<td>includes phishing, ransomware/malware and skimming</td>
</tr>
<tr>
<td>Employee error</td>
<td>includes negligence/improper disposal/loss</td>
</tr>
<tr>
<td>Accidental web/Internet exposure</td>
<td></td>
</tr>
<tr>
<td>Insider theft</td>
<td></td>
</tr>
<tr>
<td>Physical theft</td>
<td></td>
</tr>
</tbody>
</table>

1 Identity Theft Resource Center (ITRC) 2019 End of Year Data Breach Report
2 FBI’s Internet Crime Complaint Center
3 Atlas VPN 2019 Gallup Poll
4 University of Southern California 2019 Consumers & Data Privacy Perceptions
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 — and can spill over to their employer. Criminals can manipulate financial, medical, government, criminal, employment records, and even use an employee’s credentials to access organizational data. This sheer breadth of misuse makes identity crimes hard to detect, and even harder to repair without the right resources.

### FAST FACT

Seven to ten percent of the U.S. population are victimized each year, and 21 percent of those experience multiple incidents of identity fraud.

SOURCE | Identity Theft and Fraud Research Brief, Center for Victim Research

---

**IDENTITY CRIME IS GROWING — AND PERVERSIVE**

- **6 MONTHS AND 100 TO 200 HOURS WORTH OF WORK**
- **SEVERE EMOTIONAL DISTRESS: 77.3% REPORTED INCREASED STRESS LEVELS**
- **CONSUMER COST: $1,343 AVERAGE LOSS PER ID THEFT INCIDENT**
- **BUSINESS BREACH COST: AVERAGE $3,533 PER EMPLOYEE AT COMPANIES WITH 500-1,000 EMPLOYEES**

SOURCE | Various Industry Stats
SOURCE | ITRC Identity Theft: The Aftermath 2018
SOURCE | U.S. Department of Justice
SOURCE | Ponemon Institute, Cost of a Data Breach Report, 2019
COMPLEXITY AND SOPHISTICATION OF IDENTITY CRIMES

Not only can identity thieves potentially gain access to checking, savings, and 401(k) accounts, they can use this information to piece together new fake identities in what is known as synthetic identity theft.

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

Lost/Stolen PII
Social Security number, date of birth, address, credit card information, etc.

75 data records are breached every second1

65 percent of U.S. enterprises experienced a data breach, with 36 percent reporting a breach in past year2

Payments Fraud
The use of an existing financial vehicle (credit card, checking account number, bank account number) to steal funds.

Median fraud amount per victim $300³

Identity Theft
The use of lost or stolen PII to takeover a victim’s account.

60 million Americans are identity theft victims4

Out-of-pocket costs related to identity fraud have more than doubled since 20165

1 Gemalto Breach Level Index
2 Thales Data Threat Report 2019
3 Javelin Strategy & Research 2018 Identity Fraud Report
4 Harris Poll
5 Javelin Strategy & Research 2019 Identity Fraud Report
THE DARK WEB AND STOLEN IDENTITIES

The dark web, known as the black market of the Internet, is estimated to comprise six percent of the World Wide Web, including:

- Encrypted sites (requiring special software to access)
- Anonymous forums and black markets
- Stolen and illegal information

Fraudsters essentially monetize their illegal behaviors by using the dark web as a clearinghouse, and data breaches are the means by which they populate their nefarious trades.

**Shopping for stolen identities**

Your account holders’ PII is valuable. Identity thieves have several tactics for getting their hands on it and trading it for ready cash on the dark web.

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

**Dark Web Value of PII**

The price of your account holder’s identity

- Passport — $18
- PayPal Login — $42
- Driver’s License — $28
- Online Banking Details — $260
- Credit Card Details — $34
- Social Media Login — $9
- Amazon Login — $30
- Full Online Identity — $1,200

SOURCE | Dark Web Market Price Index 2019, Top10VPN
Still, stolen identities traded on the dark web are the spawning ground for a number of identity crimes, including:

- **Synthetic identity theft**, named the fastest-growing financial crime by the U.S. Department of Justice. Fraudsters use a stolen Social Security number combined with a fake name and address to open credit cards or bank accounts, apply for jobs, or obtain health insurance.

- **Credential stuffing**, the use of automated systems to process vast amounts of less secure data (think stolen emails and passwords) in an attempt to gain access to online accounts. Akamai reports there are more than 100 million fraudulent sign-on attempts daily.

- **Unsecured data**, which creates the potential for exposure and theft until a security lapse is corrected. Cloud data providers require customers to provide their own cybersecurity, but there is little standardization of application security, database controls, and other software deployments across the industry.

## Not All Data Breaches That Hit the News Are Cause for Alarm

The sensitivity of a data breach depends on a number of related factors:

<table>
<thead>
<tr>
<th>Size</th>
<th>Type</th>
<th>Timeline</th>
<th>Notification</th>
</tr>
</thead>
<tbody>
<tr>
<td>How large is the impacted population, or number of records involved?</td>
<td>How sensitive is the information; is it easily replaceable?</td>
<td>How long was the date exposed; how soon was vulnerability fixed?</td>
<td>Were you personally notified your data was included in the breach?</td>
</tr>
</tbody>
</table>
CONSUMER BEHAVIOR POST-FRAUD

28 PERCENT of account holders switch financial institutions post-fraud incident\(^1\), and most will make a change within SIX MONTHS.\(^2\)

\(^1\) PaymentsSource. As Payment Fraud Spikes, Involving Customers Can Aid Prevention

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.

**Switched Forms of Payment**
- Checking account fraud victims: 4%
- Credit card fraud victims: 13%
- All fraud victims: 22%

**Switched Primary Financial Institution**
- Checking account fraud victims: 5%
- Credit card fraud victims: 13%
- All fraud victims: 16%

**FAST FACT**
More than 85 percent of consumers agree that their identity is the most important thing they own.

SOURCE | 2019 Identity Protection Market Research Report, Sontiq

SOURCE | Javelin Strategy & Research, Understanding Post-Fraud Bank Switch
Protection of account holders’ funds can be viewed as the fundamental promise of banking.

### A PARTNER IN FIGHTING FRAUD

#### Top American Concerns

<table>
<thead>
<tr>
<th>Rank</th>
<th>Concern</th>
<th>Concerned</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Identity theft</td>
<td>61%</td>
</tr>
<tr>
<td>2</td>
<td>Bankcard fraud</td>
<td>59%</td>
</tr>
<tr>
<td>3</td>
<td>Virus/hacking</td>
<td>58%</td>
</tr>
<tr>
<td>4</td>
<td>National security</td>
<td>57%</td>
</tr>
</tbody>
</table>

Nearly 9 in 10 U.S. consumers are extremely or very concerned about at least one security area affecting their lives both online and offline.

#### Top 5 Parties Consumers Expect to Resolve an Identity Theft Incident

<table>
<thead>
<tr>
<th>Party</th>
<th>Expected to Resolve</th>
</tr>
</thead>
<tbody>
<tr>
<td>I'd have to take care of it myself</td>
<td>36%</td>
</tr>
<tr>
<td>My bank/credit card company</td>
<td>34%</td>
</tr>
<tr>
<td>The merchant responsible for the issue</td>
<td>8%</td>
</tr>
<tr>
<td>I have no idea</td>
<td>5%</td>
</tr>
<tr>
<td>Law enforcement</td>
<td>4%</td>
</tr>
</tbody>
</table>

Consumers See Themselves and Their FI as Partners in Fighting Fraud

Clearly, customers believe their bank or credit card company should be held accountable for handling the resolution process and consider their FI a primary resource for fraud protection. However, FIs are limited in their ability to provide protection against fraud that occurs outside their walls.
Most people connect identity theft with direct financial losses — but the negative consequences of having an identity stolen are also highly emotional. In fact, in a recent Sontiq survey, nearly 90 percent of respondents ranked stress and depression as the two top negative effects of their incident. Financial Loss ranked third on the list, at just 16 percent.

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

### The Impact of Identity Theft

<table>
<thead>
<tr>
<th>Experience</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Experienced General Stress</td>
<td>51%</td>
</tr>
<tr>
<td>Reported Emotional Stress/Depression</td>
<td>37%</td>
</tr>
<tr>
<td>Suffered Financial Losses</td>
<td>16%</td>
</tr>
<tr>
<td>Experienced Physical Distress</td>
<td>7%</td>
</tr>
</tbody>
</table>

**SOURCE | 2019 Identity Protection Market Research Report, Sontiq**

### What are the Must-Haves for an Identity Theft Protection Provider?

<table>
<thead>
<tr>
<th>Service</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resolve identity theft issues if/when they happen</td>
<td>84%</td>
</tr>
<tr>
<td>Notifying me of breaches that may impact my identity</td>
<td>83%</td>
</tr>
<tr>
<td>Checking my credit reports</td>
<td>68%</td>
</tr>
<tr>
<td>Check fraud protection</td>
<td>64%</td>
</tr>
<tr>
<td>Monitoring where my phone, email, and usernames are being used online</td>
<td>50%</td>
</tr>
<tr>
<td>Providing tips and guidance for protecting my identity</td>
<td>41%</td>
</tr>
</tbody>
</table>

**SOURCE | 2019 Identity Protection Market Research Report, Sontiq**
Adding identity theft and mobile threat protection into the mix offers a comprehensive solution for consumers that meets the needs of your Financial Institution.

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

Mobile devices are especially vulnerable to cyberattacks, and are responsible for at least 30 percent of all breaches, according to a 2019 Verizon report. One wrong tap from a customer or employee can download ransomware, install malware, or expose their user credentials. It's easy to see how our mobile-first culture has ushered in a major gateway to security events, considering how frequently they are leveraged to manage finances and perform work functions.

Detection is a critically important element of reacting to breaches. From your bank's mobile app through its web-based dashboard, being able to spot suspicious activity is a critical first step to alert customers that something is wrong.

FAST FACT

Hundreds of millions of people already access their financial accounts via their smart phones — a number that could grow to 3 billion by 2021.

SOURCE | Juniper Research
Fraudsters use many methods to obtain personal and confidential information. Sontiq continuously 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 black markets of the internet, we're constantly on the lookout for red flags and bad actors.

John chose to safeguard his family against the financial and emotional impact of identity theft, enrolling in an identity theft protection package.

"With all the scary stuff out there after us, it's good to know we have someone looking out for our information. This is great peace of mind for our family." —John A.
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 Sontiq 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 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.

Javelin’s most recent data reveals 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
• Mobile threat detection
• Secure online identity vault, digital wallet and password manager

Sontiq helps 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 Restoration will take care of me." — Jason C. Case #31758
We call it EZShield Restoration, a proprietary, comprehensive approach to identity restoration 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:

- **Asking valuable questions** to determine critical details of your fraud or identity theft event
- **Determining how best to assist you** with your unique situation
- **Examining your account**, your payment practices and information security habits to develop an action plan
- **Pulling your credit reports and making phone calls** to all necessary parties (including creditors and governmental organizations)
- **Providing you with vital proactive steps** to help reduce the risk of repeat fraud

A partnership with Sontiq puts 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
- **67% of victims** feel a sense of powerlessness or helplessness

*SOURCE | ITRC, Identity Theft: The Aftermath 2018*
Sontiq’s Breach RapidResponse Program helps to minimize the financial and reputational impact in the event sensitive customer information, such as Social Security numbers or account numbers, is compromised.

Here are just a few of the many things we do to help you:

- Provide tailored Identity Theft Protection solutions for your breach victims
- Get you in front of a team of Data Breach Experts that handles all the details
- Assist with formal notifications to those impacted
- Identity, privacy, and credit protection with 24/7 phone support for victims
- Access to EZShield Restoration services to help any victims of identity theft restore their good name

Sontiq also provides a Breach Readiness Program, featuring comprehensive Identity Theft Protection coupled with breach preparedness materials.

You’ll benefit from:

- Gaining access to top-rated Identity Theft Protection solution for your impacted breach victims
- Educating staff with expert-developed materials
- Compliant and efficient breach response, including custom notification letters and victim services

Main causes of security breaches

- **48% MALICIOUS OR CRIMINAL ATTACK**
- **27% HUMAN ERROR**
- **25% SYSTEM GLITCH**

SOURCE | Verizon Mobile Security Index 2019
Even with the best safeguards in place, no one can completely protect against having their identity compromised. That's where EZShield Restoration, Sontiq’s world-class, fully managed identity restoration services, comes in. When fraud happens, our team of understanding experts walks victims through the resolution process to get their life back on track and help protect against future threats.

AWARD-WINNING CUSTOMER SERVICE

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.
Sontiq works directly with you to create an integrated communication program that’s based on your goals and branded to your specifications, so you can deliver the right message at the right time to your account holders.

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

FAST FACT
Seventy-four percent of Americans say it is more important for people to have the ability to keep things about themselves that might be potentially damaging from being searchable online.

SOURCE | PEW Research Center Survey, 2019
IDENTITY PROTECTION IS ENHANCED THROUGH PERSONALIZED COMMUNICATIONS

Tailor your message based on the traits and behaviors of your buyer audience.

**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
Fraudsters are always seeking new opportunities to steal personal and financial information. That's why Sontiq 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 Sontiq could be the ideal identity protection partner for your financial institution.
Mobile Defense Suite

Security-as-a-Service for Small Businesses.

Safeguards Against Potential Cyber Threats & Data Breaches

- Dark Web Monitoring
- Account Takeover Monitoring
- Mobile Device Threat Management

Learn More