TIMES ARE CHANGING

We know consumers want to be empowered to protect themselves and everything they’ve built, and they need to understand how and when a data breach impacts them directly in order to protect what matters most. Here are some resources to start using today:

- **ID THEFT RESOURCE |** Use the Breach Clarity tool to understand the risk you face when impacted by a data breach
- **EMAIL COMPROMISE TOOL |** Track your email address at HaveIBeenPwned to see if it’s been compromised as part of a breach
- **CONSUMER TIPS & EDUCATION |** Stay current with the latest information on identity scams and fraud protection with Fighting Identity Crimes Personal Protection Articles and IdentityForce Consumer Blog
- **9 TIPS FOR BREACH VICTIMS |** Download this infographic for recommended actions to take if your identity has been impacted by a data breach

INTRODUCTION

You might feel pretty confident that you can easily navigate today’s volatile digital environment in the wake of the daily data breaches and cybercrimes. What we’re seeing here at Sontiq is actually fatigue and indifference to breach news. Not every breach requires top tier media attention and consumer protection. However, we’re all recognizing the fact that there is no way to stop or completely prevent security incidents from happening at such a rapid clip. The public is desensitized, and as a result, personal and confidential information is being left exposed to theft and fraud. And when something does happen, victims are left on their own to repair the damage to what they’ve spent their entire life building.

In the first edition of *Protecting What Matters Most*, we explored the core areas of identity theft. A year later, in the second edition, we expanded our view to provide actionable items to protect yourself further. This year, we have completely reimagined what *Protecting What Matters Most* means — to become less vulnerable.

We need to start thinking differently about our identities, including whom we trust — and whom we shouldn’t — with our personal information, while also being prepared for the inevitable: a cyber or identity crime that can spiral into weeks, months, and years of recovery. Our third edition of our *Protecting What Matters Most* eBook provides a wealth of knowledge to help frame the landscape of what we should all be paying attention to when it comes to the security and privacy of our data in a constantly evolving digital world.

OWNING AN IDENTITY IS A SERIOUS RESPONSIBILITY — AND WE’RE GIVING YOU THE TOOLS TO TREAT IT THAT WAY.

Sincerely,

Dale Dabbs | President & CEO | Sontiq
WHAT MAKES YOU, YOU
A lot goes into making us who we are. Here are some increasingly popular elements that can be used to identify you:

**BIOMETRICS**
Voice signatures, retinal scans, facial geometry, fingerprints, and DNA

**PROPERTY**
Your car’s VIN number or license plate, or title on a home or business, tax records

**HEALTH RECORDS**
Medical ID number, health insurance data, patient records, prescriptions

**SOCIAL MEDIA**
Profile handles, photos, geo-location, connections, interests

Identities are personal, clearly, just as much as the elements that make up our identities are unique. From our physical appearance to where we work and our ethnicity — to also our Social Security numbers (SSN), medical ID numbers, and fingerprints. And, criminals know how to capitalize on every component of our identity to commit fraud.

Businesses have identities, too, from Employer Identification Number (EIN) to D-U-N-S Number, and these elements are just as susceptible to theft and fraud and impact more than just the business — a security incident compromises the confidential information of customers, partners, and employees.

**CONSIDERING WHAT IS AT STAKE, SECURING THESE PERSONAL OR BUSINESS IDENTIFIERS SHOULD BE TOP OF MIND. SO, WHY AREN’T THEY?**

Frankly, most of us don’t realize just how often our sensitive personal data is collected or where it lives, never mind who is responsible for protecting it. Our data represents an intelligence goldmine for the companies that want to market and sell their products — and they’re willing to pay for it — to the tune of $19 billion. That’s how much U.S.-based companies spent to collect and analyze consumer data in 2018, according to the Interactive Advertising Bureau. It may be easier to avoid thinking about our digital identities at scale. Or, just accept the tradeoff, that we may be providing too much personal information and not really linking that to why we’ve all become more vulnerable — especially as we’re constantly flooded with the latest cyber threat du jour. *But we need to.*

No matter what stage of life we’re in, whether as individuals or a growing business, identity theft impacts everyone. Victims’ relationships with family, friends, coworkers, employees, bosses, and customers all become strained due to physical and financial stress, mitigation and remediation cost, and even broken trust. It’s our responsibility to protect these relationships by protecting the identity of ourselves and those in our support systems.

**LOST PRODUCTIVITY**
6 MONTHS and 100 to 200 Hours Worth of Work

**SEVERE EMOTIONAL DISTRESS**
77% Reported INCREASED Stress Levels

**CONSUMER COST**
Average LOSS of $429 Per ID Theft Incident

SOURCE | Various Industry Stats
SOURCE | ITNC Identity Theft: The Aftermath 2018
Identity theft is a lifelong threat, but some identities are more prone to attack. Children fall into this category with over 1 million having their identity stolen annually. Recent data also shows that two-thirds of victims are only 8 years old or younger. And, because children's data isn't typically monitored for suspicious activity, the fraud can go undetected for many years, making our youngest population the most appealing to identity thieves.

How does child ID theft happen? Well, a cybercriminal can infiltrate the network of a pediatrician’s office and steal the Personally Identifiable Information (PII) — names, dates of birth, and Social Security Numbers — of hundreds of children. They can use this data to perpetuate synthetic identity theft, creating an entirely new identity based on pieces of real information, to apply for government benefits, open credit cards, take out loans, or seek employment.

In an even more terrifying scenario, cybercriminals are selling off children's datasets in bulk on the Dark Web, the anonymous areas of the internet where buying and selling of illegal information dominates and that can only be reached with special web browsers. These child ID packages are called “fullz” — a slang term for a file that contains enough elements of victims’ identity to commit fraud.

On the other end of the identity theft lifecycle, seniors represent the second-most vulnerable, and fastest-growing population targeted by scammers and ID thieves. Fraudsters prey on their trusting nature and unfamiliarity with technology to con the elderly out of cash, personal or medical information, or even retirement account numbers.

Older adults have accumulated a life’s worth of assets, they usually have little debt to their names, and are less likely to use credit. Just like child identity theft, senior fraud may go undetected, if not monitored regularly.

When a family member experiences a violation like identity theft, it affects everyone in the household. We can’t afford to leave our children’s futures, or everything we’ve built, at risk.
As we mentioned earlier, owning an identity is a serious responsibility — and businesses have the added pressure of protecting the information of not only the business, but also its employees, customers, and partners. There are 30.2 million Small and Medium-sized Businesses (SMBs), defined as companies with less than 500 employees, operating in the United States. And, SMBs employ almost half of working adults, according to the U.S. Small Business Administration.

When businesses grow, the data they are responsible for protecting increases as well. Cybercriminals have taken notice, and SMBs have become one of their favorite targets for stealing data or using them as a stepping-stone to infiltrate larger enterprises. Business networks are generally much larger than an individual’s, meaning customers, vendors, partners, employees, family members — essentially everyone tied to the company — may be negatively impacted by an identity crime.

Small businesses experience the majority (58%) of DATA BREACHES, AND 67% have faced a CYBER ATTACK in the last 12 months.

**BIGGEST CYBERSECURITY THREAT**

Employee negligence remains the leading cause of data breaches, according to a Shred-it report.

SMBs appear to be indifferent and desensitized toward the inevitability of a malicious attack. This reinforces the need to pay attention to the details that matter so we are all less vulnerable.

48% of small businesses think they are TOO SMALL to be a target of online fraud.

65% FAIL TO ACT following a cybersecurity incident.

72% are NOT CONFIDENT in their ability to combat the cyber risks they face.
Every personal or professional interaction we have leaves a trail of data. Modern devices collect and share your information to analyze your behavior and interests, with the intent to personalize every digital experience. In our “smart” homes we have thermostats, TVs, security systems, lighting, appliances, and virtual assistants. We connect to the Internet through our cars and navigate our way using GPS systems. And, with our every movement, our smartphones and fitness apps trace our steps and record our biometric data.

All of this information helps to comprise the Internet of Things (IoT) and paints a powerful digital picture of who we are, what we’re doing, and where we’ve been — even where we’re likely to go next. It’s why we need to pay attention to what is collected, who is using it, and what threats its exposure may pose to you, your family, or your business.

Threats from IoT devices have always exposed consumers to identity theft and fraud, but it’s not just individual identities being endangered by these smart devices.

### AT HOME

Request a copy of your IoT device recordings, such as those from Amazon Alexa

Adjust your social media privacy settings

Test your password strength, and sign up for a password manager to keep them secure

### FOR EMPLOYERS

Invest in mobile threat defense to monitor employee devices for risks to your network

Make sure any enterprise devices you use adhere to the National Institute of Standards and Technology’s (NIST) guidance for IoT devices to only perform their intended functions and avoid unintentional data collection

Prepare a data breach response plan so that everyone knows what to do if the worst were to happen

IT security professionals rank MOBILE DEVICES as the HARDEST THREAT to defend against, with 74% saying they’ve directly led to a DATA BREACH.

SOURCE | Buying Into Mobile Security, IDG

### TESTING THE FENCES

Here are a few examples of how cybercriminals are reimagining ways to turn devices against businesses, hospitals, and government agencies:

- IoT devices can be weaponized in disruptive Distributed Denial of Service (DDoS) attacks that block online services and wreak havoc on operations.
- Employees’ smartphones are being targeted with phishing attacks to install malware on network servers.
THINKING DIFFERENTLY

WE CAN ALL BE LESS VULNERABLE

Awareness is the first step in addressing any problem. We know there are a multitude of ways fraudsters compromise us, our family members, and our businesses, and now’s the time to start thinking differently about how our identities are intertwined with our digital lives.

To become less vulnerable, we must use caution about where, when, and with whom, we share our personal information.

TAKE THIS QUIZ TO DETERMINE YOUR VULNERABILITY

Tally the red answers to determine your risk level
1 – 3 = Low Risk
4 – 6 = Moderate Risk
7 – 10 = High Risk

1. Do you receive alerts to stay aware of the latest consumer scams? The FTC publishes scam alerts and you can sign up for email updates.
   YES  NO
2. Have you received a data breach notification in the past 12 months? One in three data breach victims later go onto experience identity crimes.
   YES  NO
3. Have you disposed of personal or financial documents in the trash? Dumpster diving and mail theft remain prevalent. Always shred sensitive documents.
   YES  NO
4. Is your Personally Identifiable Information (PII) on the Dark Web? Identity protection services may include a Dark Web scan so you can find out if your PII is for sale.
   YES  NO
5. Have you removed yourself from public databases? Data brokers collect and share our information without our knowledge. Opt out here.
   YES  NO
6. Does your employer collect data on your work performance? More than half of businesses do not ask for consent to do so. Talk with your HR or IT leaders to understand what information is being collected, how it’s used, and how it’s protected.
   YES  NO
7. Do you know what permissions you’ve granted your mobile apps? Many can access your microphone, camera, etc., and share with third parties. Check your app settings and restrict unnecessary access.
   YES  NO
8. Have you received a phishing email at work? Even if you recognized the signs and didn’t click, there’s a chance that one of your colleagues or family members may have. Be proactive anytime you suspect a phishing scam.
   YES  NO
9. Is your payment card or bank account tied to a mobile payment app? Use a passcode on your device and strong passwords for each bank account. If your device is lost or stolen, contact your bank and disconnect mobile access from your accounts.
   YES  NO
10. Have you shared your Social Security Number over the phone? 48 billion robocalls were made in 2018, with 37% of those known to be scams. Remember, if you get a legitimate call from the U.S. government, they will not require you to provide your SSN over the phone.
   YES  NO
WANT TO LEARN MORE?

THE BALANCE SMALL BUSINESS
What is Your D-U-N-S Number?
https://www.thebalancesmb.com/what-is-my-dandb-number-393461

BLOCK ADVISORS
Small Business Identity Theft: Warning Signs and Protective Measures

BUSINESSIDTHEFT.ORG
What is Business Identity Theft?

THE BUSINESS JOURNALS
Amazon's Alexa Approved to Share HIPAA-Regulated Health Information

CAMPAIGN FOR A COMMERCIAL-FREE CHILDHOOD
Alexa, What are You Doing with Kids' Data?
https://commercialfreechildhood.org/blog/alexa-what-are-you-doing-kids-data

CBS NEWS
I Asked Alexa and Google Assistant How to Find My Data. Here's What They Said

CENTER FOR RURAL AFFAIRS
Five Signs of Small Business Identity Theft

CHECK POINT RESEARCH
Under the Hood of Cyber Crime: The Rise of Stealthy and Targeted Cyber Attacks

CHICAGO TRIBUNE
When Alexa Listens, It Records. Amazon Wrongly Sent One Home's Alexa Archive — 1,700 Audio Files — to a Stranger

CIO
6 Steps to a More Secure IoT
https://www.cio.com/article/3385059/6-steps-to-a-more-secure-iot.html

CNBC
The Biggest Cybersecurity Risk to US Businesses is Employee Negligence, Study Says
Companies are Collecting More Data on Employees, and Not All Confident They are Doing it Responsibly

CNN
The Real Danger of Alexa Listening to Our Convos

CSO
7 Mobile Security Threats You Should Take Seriously in 2019
The Internet of Things (IoT) — Threats and Countermeasures

CYBERSECURITY VENTURES
60 Percent of Small Companies Close Within 6 Months of Being Hacked
https://cybersecurityventures.com/60-percent-of-small-companies-close-within-6-months-of-being-hacked/
DOGTOWN MEDIA
The Most Common IoT Cybersecurity Threats of 2019

DUN & BRADSTREET
What is a D-U-N-S Number?
https://www.dnb.com/duns-number.html

ERICSSON
The Internet of Things Forecast

EXPERIAN
Child Identity Theft Campaign Overview

FAST COMPANY
Supreme Court Rejects Amazon’s Zappos on Data Breach Lawsuit

FEDERAL TRADE COMMISSION
Child Identity Theft
https://www.consumer.ftc.gov/articles/0040-child-identity-theft

Children’s Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business

Fake Calls About Your SSN
https://www.consumer.ftc.gov/blog/2018/12/fake-calls-about-your-ssn

Most Recent Scam Alerts
https://www.consumer.ftc.gov/features/scam-alerts

Scams Against Older Adults: Reporting to Congress

Starting Today, New Federal Law Allows Consumers to Place Free Credit Freezes and Yearlong Fraud Alerts

FORBES
A Business is a Living Entity — How Do You Keep it Breathing?
https://www.forbes.com/sites/forbestechcouncil/2018/03/07/a-business-is-a-living-entity-how-do-you-keep-it-breathing/#1b1a0a9b2192

Amazon Slammed for Putting Kids at Risk with ‘Blatant Violation of Privacy Laws’

Why There’s a More Important Wall that Needs to Be Built at Our Digital Border

GADGET HACKS
5 Ways to Keep Google from Collecting Data on Your Android Phone
https://android.gadgethacks.com/how-to/5-ways-keep-google-from-collecting-data-your-android-phone-0181002/

THE HILL
Twenty Years of Children’s Online Privacy Success Provides Blueprint for Comprehensive Public Policy
https://thehill.com/opinion/technology/412587-twenty-years-of-childrens-online-privacy-success-provides-blueprint-for

HISCOX
2018 Hiscox Small Business Cyber Risk Report

IDENTITY THEFT RESOURCE CENTER
2018 End-of-Year Data Breach Report

2019 Trends and Predictions for Identity Theft, Data Privacy and Cybersecurity

The Aftermath: The Non-Economic Impacts of Identity Theft
https://www.idtheftcenter.org/aftermath2018/

INTERNET LIVE STATS
In 1 Second, Each and Every Second, there are...
https://www.internetlivestats.com/one-second/
IOT FOR ALL
The 7 Most Common IoT Security Threats in 2019
https://www.iotforall.com/7-most-common-iot-security-threats-2019/

JAVELIN STRATEGY & RESEARCH
2018 Child Identity Fraud Study
Child Identity Theft Hit More Than One Million U.S. Victims in 2017
https://www.javelinstrategy.com/node/59561

KREBS ON SECURITY
Target Hackers Broke in Via HVAC Company

MAYER BROWN
President Trump Launches AI Strategy for Federal Government

MERITALK
NIST Drafts IoT Security Guidance for Home and Small-Business Devices

MONEY
Here's How Facebook or Any Other App Could Use Your Phone's Microphone to Gather Data

NATIONAL CONFERENCE OF STATE LEGISLATURES
Data Security Laws | Private Sector

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)
Securing Small-Business and Home Internet of Things (IoT) Devices

THE NEXT WEB
The Worrying Trend of Children's Data Being Sold on the Dark Web

NINJA RMM
7 Eye-Opening Cybersecurity Statistics Every Small Business Needs to Know in 2019

PONEMON INSTITUTE
2018 State of Cybersecurity in Small & Medium Size Businesses

PRIVACY RIGHTS CLEARINGHOUSE
Data Breaches
https://www.privacyrights.org/data-breaches

PROOFPOINT
Global Cybersecurity Awareness Study Reveals 33 Percent of U.S. Respondents Have Experienced Identity Theft, More than Twice the Global Average

PYMNTS.COM
Amazon Wants Alexa to Track Medicine, Provide Health Data

QUARTZ
Your Phone Conversation Isn't Really Spying on Your Conversations — The Truth Might Be Even Creepier
https://qz.com/1609356/your-phone-is-not-recording-your-conversations/

SECURITY BOULEVARD
Identity Theft and Financial Fraud in the Digital Age
SECURITY INTELLIGENCE
Data Breach Fatigue Makes Every Day Feel Like Groundhog Day
https://securityintelligence.com/data-breach-fatigue-makes-every-day-feel-like-groundhog-day/

SIGNATURE ANALYTICS
Employee Fraud is More Common in Small Businesses — Are You Protected?

SMALL BUSINESS TRENDS
48% of Businesses Think They’re Not Big Enough to Be Targeted for Fraud

TECHCRUNCH
Smart Home Tech Makers Don’t Want to Say if the Feds Come for Your Data

TECHJURY
How Many IoT Devices are There?
https://techjury.net/blog/how-many-iot-devices-are-there/

TECHRADAR
Are Our Phones Listening to Us?
https://www.techradar.com/news/are-our-phones-listening-to-us
Evolution of Fraud in the IoT Era

UBUNTUPIT
25 Most Common IoT Security Threats in an Increasingly Connected World

U.S. SMALL BUSINESS ADMINISTRATION
2018 Small Business Profile

VERIZON
2019 Data Breach Investigations Report
https://enterprise.verizon.com/resources/reports/dbir/

VICE
Children’s Personal Data & SSNs Are Being Sold on the Dark Web

THE WASHINGTON POST
Alexa Has Been Eavesdropping on You this Whole Time
https://www.washingtonpost.com/technology/2019/05/06/alexa-has-been-eavesdropping-you-this-whole-time/?noredirect=on&utm_term=.359b4168957c
Report: Occupational Fraud is Siphoning ‘Staggering Amounts’ of Money from Small Businesses

WBRC
Has Your Child’s Identity Been Stolen? Find Out How to Protect Their Personal Information
https://www.wbrc.com/2019/04/19/has-your-childs-identity-been-stolen-find-out-how-protect-their-personal-information/

ZDNET
I Asked Apple for All My Data. Here’s What was Sent Back
“Given the inevitability of data breaches, the sophistication of cyber thieves, and the harmful impact identity crime has on businesses and individuals; IDENTITY THEFT PROTECTION IS AN INTEGRAL PART OF A ROBUST CYBERSECURITY STRATEGY.”

Stacey Smith, President & CEO

“Our identities are the keys to so many different services, and that has made data breaches a fact of life in today’s digital world. But fraud is not an inevitability if we each take action. FRAUDSTERS ONLY SUCCEED WHEN WE DON’T FIGHT BACK.”

AL PASCUAL, COO

ABOUT SONTIQ

Sontiq, headquartered in Nottingham, MD, is a high-tech security and identity protection company arming businesses and consumers with award-winning products built to protect what matters most. Sontiq’s brands, EZShield and IdentityForce, provide a full range of identity monitoring, restoration, and response products and services that empower customers to be less vulnerable to the financial and emotional consequences of identity theft and cybercrimes. Learn more at www.sontiq.com or engage with us on Twitter, Facebook, LinkedIn, or YouTube.