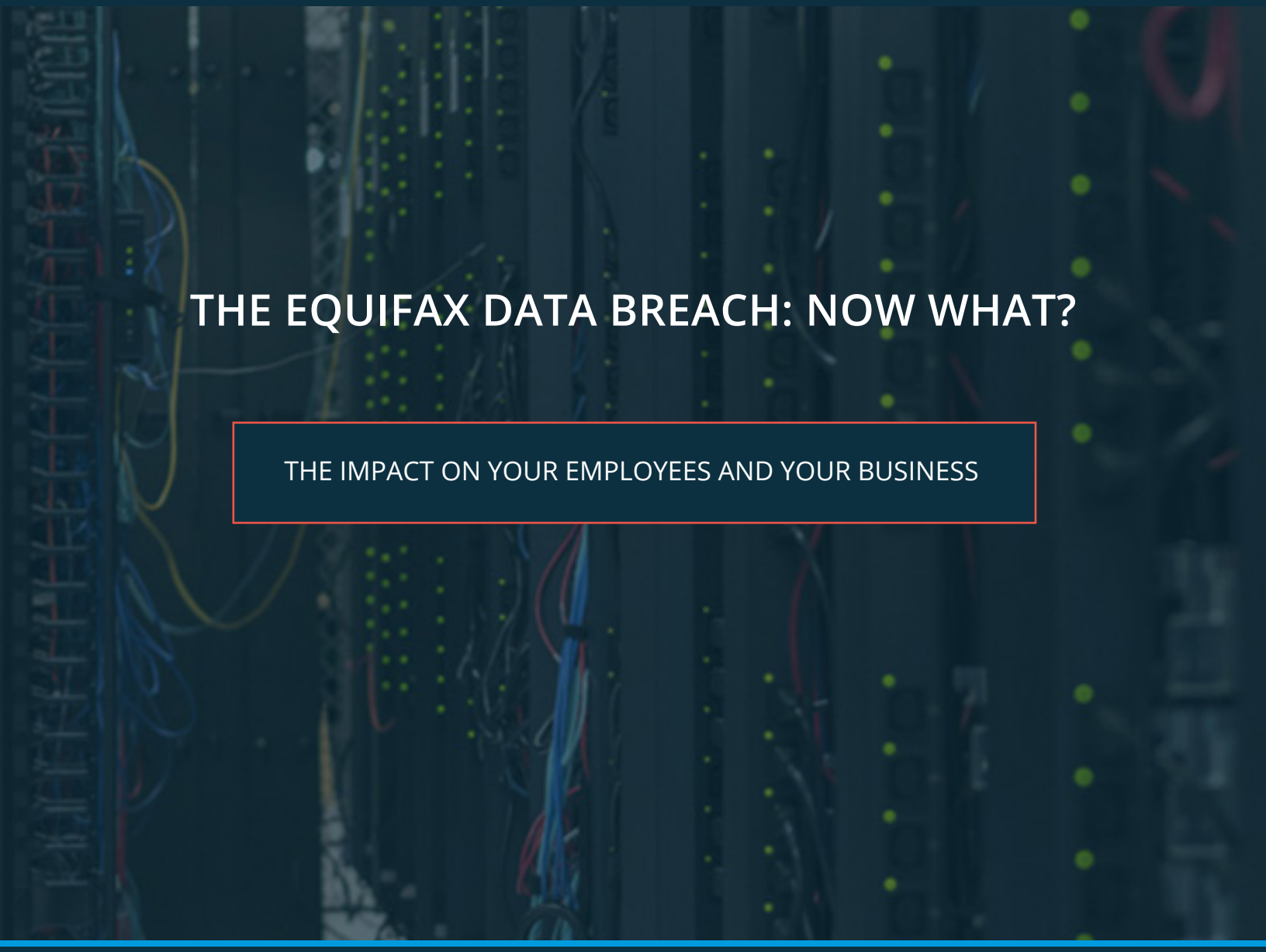
IdentityForce™

A BUSINESS HANDBOOK



THE EQUIFAX DATA BREACH: NOW WHAT?

THE IMPACT ON YOUR EMPLOYEES AND YOUR BUSINESS

Published | September 2017

DATA BREACH IMPACT

Approximately 143 million Americans, or nearly half of the U.S. population, had their personal data exposed in the Equifax cyber incident between mid-May through July 2017, according to the company.[1] What made this data breach so much more devastating than garden-variety hacks was that the crown jewels of personal identity — Social Security Numbers (SSNs), names, and dates of birth — were stolen. This information is likely to remain unchanged forever for most victims, which extends the risk for consumers virtually in perpetuity. As a result, there will undoubtedly be significant, potentially negative ripple effects across your company's customers and employees for years to come.

MAJOR DATA BREACHES BY THE NUMBERS

Although the Equifax data breach was not the largest theft of personal information, it may be the most potentially damaging. Here are some quick facts about other major data breaches:

- In May 2014, Yahoo reported the theft of 500 million Yahoo user accounts, including names, email addresses, telephone numbers, dates of birth, and, in some cases, encrypted and unencrypted security questions and answers, according to a 2016 USA Today report.[2]
- Myspace reported a breach of 360 million user accounts and LinkedIn exposed 100 million users to potential identity theft risk in May 2016. They join a long dateline of damaging hacking attacks over the past decade, from AOL (October 2007) to JP Morgan Chase (October 2013) and from Target (November 2013) to Anthem (February 2015).[3]

Breached Data: The Crown Jewels of Personal Identity

Information that was likely compromised in the Equifax data breach includes:

- **Social Security Numbers (SSNs)**
- **Driver's license numbers**
- **Full names**
- **Dates of births**
- **Addresses**
- **Credit card numbers for 209,000 customers**

1. "Equifax Releases Details on Cybersecurity Event, Announces Personnel Changes," Equifax.com press release, September 15, 2017.
2. "500 million Yahoo accounts breached," USA Today, September 22, 2016.
3. "Yahoo may be the biggest data breach," USA Today, September 22, 2016.

WHAT BUSINESS LEADERS NEED TO KNOW

A major cause for concern with the Equifax event was the 40-day delay in making the public aware of the intrusion, per media reports. (At the time of this writing, there are some reports that a second major Equifax breach occurred in March 2017.) The gap between detecting the theft and Equifax's management team announcing it to the public on September 7th was due to several factors. The company most likely needed to patch vulnerabilities in its security infrastructure, determine the scope of how much data was stolen, and inform law enforcement officials who no doubt wanted time to try to identify the hackers before the company released information. In the interval, the criminals likely could cover or at least obscure their digital tracks — making detection and capture that much more difficult.

Equifax's crisis response plan also invited controversy. It included creating a website so that those potentially exposed to the breach could confirm whether their personal information was compromised. They also offered consumers a free credit freeze and time-limited free membership to TrustedID, a suite of Equifax's own security products.

Beside the fact that consumers may be leery of using Equifax, there are also several major structural problems with Equifax's response. First, a credit freeze is just a tool. It's not a solution designed to protect employees or individual consumers from identity theft. In addition, the credit freeze that Equifax is offering only applies to its credit bureau — it does not address user activity at Experian and TransUnion, the other two major U.S. credit monitoring services.

Second, the Equifax package is significantly limited, as it is only focused on credit. It does not directly address or protect consumers from the massive fallout of having a compromised personal identity. According to IdentityForce's CEO, Steven Bearak, "Credit fraud only makes up 28% of identity theft risk. If all the consumer does is freeze their credit, they haven't addressed the other 72% of identity theft activities that could affect them, from health insurance fraud to pilfering of awards points — scams for which there is an active, mature, and lucrative black market, especially within the Dark Web."

"Credit fraud only makes up 28% of identity theft risk. If all the consumer does is freeze their credit, they haven't addressed the other 72% of identity theft activities that could affect them, from health insurance fraud to pilfering of awards points — scams for which there is an active, mature, and lucrative black market, especially within the Dark Web."

— Steven Bearak, *CEO, IdentityForce*

What should not be lost in discussions about the scope of the Equifax data breach and the company's response is the immutable fact that Personally Identifiable Information (PII) of 44% of the US population has been jeopardized. In the months and years to come, this could have a seriously detrimental impact on the economy and on businesses that rely on employees and customers trusting that their PII will be safeguarded.

DISRUPTION TO YOUR EMPLOYEES: A SERIOUS PRESSURE COOKER

For an American workforce that is already anxious about protecting their personal information and coping with financial stress, the Equifax breach undoubtedly cranks up the pressure. Not only can thieves potentially gain access to checking, savings, and 401(k) accounts, they can use this information to piece together new fake identities, known as synthetic identity theft.

Again, the numbers tell a harrowing story:

- Identity theft is a major catalyst for long-term stress, as 66% of all data-breach victims reportedly experience direct financial losses.[4]
- 48% of respondents in a recent survey believe that their identity was at risk for years after a single data-breach incident.[5] This percentage is likely to skyrocket in the wake of the Equifax data breach.
- Identity theft has been identified as the 8th biggest fear among Americans, exacting a significant toll on their confidence and emotional state both at home and at work.[6]

The impact to business productivity and profits related to data breaches can be significant. The downtime for employees who need to confirm the integrity of their identity, or go through the complex process of repairing a stolen identity, is estimated to range from 33 to 600 hours.[7] This takes a real toll on employees' emotional states, and can lead to health issues including significant personal stress, chronic anxiety, and frustration. Your business results may also suffer from an erosion of trust, as employees may be on edge and suspicious of how well you protect their personal data.

This message is clearly resonating with human resources professionals, as revealed in IdentityForce's State of Progressive Employee Benefits Survey of 105 HR professionals. The survey showed that 55% of respondents already are, or might consider adopting, identity theft protection, and 22% of those considering it plan to do so in the next 12 months.[8] A separate employee benefits study published by the Society of Human Resource Management (SHRM) revealed that, for the first time in 2017, 9% of its members provide paid identity protection for their employees.[9]

55% of those surveyed already are, or might consider adopting, identity theft protection

Source: IdentityForce's State of Progressive Employee Benefits Survey (September 2017)

4. Small Business Trends blog post, "Keep it Down! Employees Rank Workplace Distractions as Biggest Beef," June 14, 2016.
5. Ibid.
6. *The Chapman University Survey of American Fears*, 2016.
7. *2016 Identity Fraud Study*, Javelin Strategy and Research, February 2016
8. For the full results, please refer to the IdentityForce Executive Summary, "Nearly 68% of HR Professionals Consider Identify Theft Protection an Increasingly Important Employee Benefit, Survey Reveals."
9. SHRM, 2017 *Employee Benefits: Remaining Competitive in a Challenging Talent Marketplace.*

A DATA BREACH IMPACTS YOUR WORKFORCE FOR YEARS TO COME

As noted above, the Equifax breach of Personally Identifiable Information (PII) is fundamentally different from most forms of identity hacking. Unlike credit cards, which can be cancelled immediately, the theft of PII is perpetual. Victims cannot cancel their SSNs. Worse yet, most of the individuals affected — who may not have done business with Equifax directly — may not even realize their data has been exposed, given the nature of the Equifax business model. Most of Equifax's business comes directly from banks who use the service to verify credit of their borrowers. Even if the banks disclose to borrowers the nature of the agency relationship, the borrowers may not be aware that their information is indefinitely stored on the servers of the agencies.

To a cyber thief, having access to millions of SSNs is the Holy Grail of digital crime. Not only can fraudulently obtained PII be quickly monetized on the Dark Web, it can be used to set up fake identities, in effect combining different names, home addresses and SSNs to defraud your employees. In fact, using the often less detectable SSNs of children and the elderly is a preferred modus operandi of cyber criminals, who can exploit this information for years while destroying the children's future creditworthiness in the process. Here are some of the ways PII can be used by these thieves:

- Setting up fraudulent bank accounts to withdraw and drain funds
- Setting up fraudulent pension or 401(k) withdrawals
- Abusing health insurance benefits
- Applying for new credit cards using fake IDs
- Filing fraudulent tax returns to claim refunds

Impact on Children

Sometimes parents provide their children's PII when setting up their credit file. Successful thieves can combine real and fake data to compile new identities. They then use these synthetic identities to obtain credit, open bank accounts, and apply for driver's licenses and passports.

STEPS FOR PROTECTING YOUR EMPLOYEES AND THEIR FAMILIES

There are six steps you and your employees can do together to help protect against identity theft:

1. **Stay vigilant** – Employees can request a free annual credit report and you should encourage them to monitor their credit card activity and bank statements. They can contact the non-profit Identity Theft Resource Center at (888) 400-5530 to get assistance with identify theft mitigation, and/or subscribe to an identity theft and credit monitoring service that will alert them when their personal information is being used.
2. **Get support** – If they are confirmed identity theft victims, they can create an Identity Theft Report with the Federal Trade Commission (FTC). Visit www.identitytheft.gov, the federal government's resource for identity theft victims, for details. Note that law enforcement likely will request a copy of any Identity Theft Report filed.
3. **Stop cyber criminals in their tracks** – Put an extended fraud alert or security freeze on your credit. An extended fraud alert, which is available up to seven years in most states, allows creditors to see someone's credit file, but they must contact him or her to identify before extending credit. A credit freeze generally prevents creditors from accessing someone's credit file.
4. **File taxes early** – Filing early protects them from identity thieves who might try to file and collect tax refunds before the employees complete those steps. Requesting a Personal Identification Number (PIN) to submit a return also adds another security layer.
5. **Contact the Social Security Administration** – By requesting a copy of their wage-earning report, your employees can verify that their Social Security Numbers are not being used fraudulently, resulting in their being liable for taxes on wages reported by someone who's stolen their information.
6. **Work with your employee benefits administrator and/or recordkeeper** – Reassure your employees that you are monitoring accounts for any suspicious retirement plan withdrawals/activity and/or medical claims. Encourage them to request a copy of their statements to further stay on top of their benefits.

MONITOR

ALERT

CONTROL

RECOVER

SELECT THE RIGHT IDENTITY THEFT PROTECTION PARTNER

IdentityForce is an established provider of identity, privacy, and credit solutions. Through our comprehensive identity protection solution, IdentityForce monitors each employee's digital footprint and detects suspicious changes in the user's personal, financial, and credit information.

Through a subscription service, our members are protected 24/7 with comprehensive monitoring. IdentityForce continuously scans both the publicly accessible portions of the Internet, as well as the hidden areas not visible publicly, known as the Dark Web, and alerts members of any suspiciously activity tied to their identity. IdentityForce provides an early warning system with rapid notification to our members' mobile devices (via email and text messaging) when the security of PII is deemed to be at risk. Should one of our members become victim of identity theft, they can rest easier knowing that they have access to fully-managed recovery services and up to $1 million of identity theft coverage.

Learn More Today!

Contact IdentityForce today to learn how we are committed to helping employers, individuals and their families, and our partners protect personal information and remove the emotional stress and hardship that identity theft can have on people everywhere.

Exclusive Breach Guarantee

If your company were to experience its own data breach, we also offer an exclusive Breach Guarantee, providing white-glove restoration services to any of your employees affected by the breach for 12 months. All at zero cost to your company!

About IdentityForce

For nearly 40 years, IdentityForce, Inc. has provided best-in-class, highly scalable, award-winning identity theft, privacy, and credit protection solutions to consumers, businesses, and government agencies. A pioneer of identity protection, IdentityForce's innovation and customer-centric approach has made the company a trusted partner for both organizations and individuals. IdentityForce also provides custom-tailored programs to organizations enabling them to build closer relationships and additional revenue streams. In 2015, the U.S. government awarded IdentityForce elite Tier-One status as an approved provider of identity protection services for data breaches affecting over 21.5 million people. Visit www.identityforce.com to learn more.

Find **IdentityForce** on:

Download on the App Store

GET IT ON Google Play