

**EXAMINING THE EQUIFAX DATA BREACH,  
CONTINUATION**

---

**HEARING**  
BEFORE THE  
**COMMITTEE ON FINANCIAL SERVICES**  
**U.S. HOUSE OF REPRESENTATIVES**  
ONE HUNDRED FIFTEENTH CONGRESS  
FIRST SESSION

\_\_\_\_\_  
OCTOBER 25, 2017  
\_\_\_\_\_

Printed for the use of the Committee on Financial Services

**Serial No. 115-50**



\_\_\_\_\_  
U.S. GOVERNMENT PUBLISHING OFFICE  
WASHINGTON : 2018

30-339 PDF

## HOUSE COMMITTEE ON FINANCIAL SERVICES

JEB HENSARLING, Texas, *Chairman*

PATRICK T. MCHENRY, North Carolina,  
*Vice Chairman*

PETER T. KING, New York  
EDWARD R. ROYCE, California  
FRANK D. LUCAS, Oklahoma  
STEVAN PEARCE, New Mexico  
BILL POSEY, Florida  
BLAINE LUETKEMEYER, Missouri  
BILL HUIZENGA, Michigan  
SEAN P. DUFFY, Wisconsin  
STEVE STIVERS, Ohio  
RANDY HULTGREN, Illinois  
DENNIS A. ROSS, Florida  
ROBERT PITTENGER, North Carolina  
ANN WAGNER, Missouri  
ANDY BARR, Kentucky  
KEITH J. ROTHFUS, Pennsylvania  
LUKE MESSER, Indiana  
SCOTT TIPTON, Colorado  
ROGER WILLIAMS, Texas  
BRUCE POLIQUIN, Maine  
MIA LOVE, Utah  
FRENCH HILL, Arkansas  
TOM EMMER, Minnesota  
LEE M. ZELDIN, New York  
DAVID A. TROTT, Michigan  
BARRY LOUDERMILK, Georgia  
ALEXANDER X. MOONEY, West Virginia  
THOMAS MacARTHUR, New Jersey  
WARREN DAVIDSON, Ohio  
TED BUDD, North Carolina  
DAVID KUSTOFF, Tennessee  
CLAUDIA TENNEY, New York  
TREY HOLLINGSWORTH, Indiana

MAXINE WATERS, California, *Ranking Member*

CAROLYN B. MALONEY, New York  
NYDIA M. VELÁZQUEZ, New York  
BRAD SHERMAN, California  
GREGORY W. MEEKS, New York  
MICHAEL E. CAPUANO, Massachusetts  
WM. LACY CLAY, Missouri  
STEPHEN F. LYNCH, Massachusetts  
DAVID SCOTT, Georgia  
AL GREEN, Texas  
EMANUEL CLEAVER, Missouri  
GWEN MOORE, Wisconsin  
KEITH ELLISON, Minnesota  
ED PERLMUTTER, Colorado  
JAMES A. HIMES, Connecticut  
BILL FOSTER, Illinois  
DANIEL T. KILDEE, Michigan  
JOHN K. DELANEY, Maryland  
KYRSTEN SINEMA, Arizona  
JOYCE BEATTY, Ohio  
DENNY HECK, Washington  
JUAN VARGAS, California  
JOSH GOTTHEIMER, New Jersey  
VICENTE GONZALEZ, Texas  
CHARLIE CRIST, Florida  
RUBEN KIHUEN, Nevada

KIRSTEN SUTTON MORK, *Staff Director*

# CONTENTS

	Page
Hearing held on:	
October 25, 2017 .....	1
Appendix:	
October 25, 2017 .....	27

## WITNESSES

WEDNESDAY, OCTOBER 25, 2017

Cable, Sara, Director, Data Privacy and Security, Assistant Attorney General, Consumer Protection Division, Office of Attorney General, Commonwealth of Massachusetts .....	4
Litt, Mike, Consumer Advocate, U.S. Public Interest Research Group .....	8
McGee, Kathleen, Chief, Bureau of Internet and Technology, Division of Eco- nomic Justice, Office of the New York State Attorney General .....	5
Moy, Laura, M., Deputy Director, Center on Privacy and Technology, George- town University Law Center .....	7
Wu, Chi Chi, Staff Attorney, National Consumer Law Center .....	6

## APPENDIX

Prepared statements:	
Cable, Sara .....	28
Litt, Mike .....	90
McGee, Kathleen .....	99
Moy, Laura, M. ....	103
Wu, Chi Chi .....	124

## ADDITIONAL MATERIAL SUBMITTED FOR THE RECORD

Waters, Hon. Maxine:	
Letter from VantageScore .....	137
New York Times article entitled, “Equifax Grip on Mortgage Data Squeezes Smaller Rivals” .....	142
Written questions for the record submitted by Democratic members for October 5, 2017 Equifax hearing .....	146
Press statement from CFPB entitled, “Supervisory Highlights Focused on Problems Discovered with Credit Bureaus” .....	160
Written statements for the record from the first Equifax hearing on October 5th .....	163
Information about ID theft tools available to consumers on CFPB’s website .....	171



## **EXAMINING THE EQUIFAX DATA BREACH, CONTINUATION**

**Wednesday, October 25, 2017**

U.S. HOUSE OF REPRESENTATIVES,  
COMMITTEE ON FINANCIAL SERVICES,  
*Washington, D.C.*

The committee met, pursuant to notice, at 2 p.m., in room 2128, Rayburn House Office Building, Hon. Ted Budd [member of the committee] presiding.

Present: Representatives Rothfus, Mooney, Budd, Waters, Maloney, Sherman, Meeks, Capuano, Clay, Scott, Green, Ellison, Perlmutter, Himes, Foster, Kildee, Sinema, Beatty, Heck, Gottheimer, Gonzalez, Crist, and Kihuen.

Mr. BUDD [presiding]. The committee will come to order. Without objection, the chair is authorized to declare a recess of the committee at any time, and all members will have 5 legislative days within which to submit extraneous materials to the chair for inclusion in the record. Pursuant to clause D-5 of rule three of the Committee on Financial Services, this additional hearing day has been scheduled with reference to October 25th, 2017, full committee hearing entitled "Examining the Equifax Data Breach."

The Chair now recognizes the Ranking Member of the committee, the gentlelady from California, for 4 minutes for an opening statement.

Ms. WATERS. Thank you very much, Mr. Chairman.

And thank you to all of the witnesses who are here today to better understand the causes and impact of the massive data breach at Equifax. State government experts and consumer advocates to testify here today, I want to thank you for being here to testify today.

Unfortunately, the CEOs of each of these three major credit bureaus have refused to attend this hearing. It is particularly troubling that since the massive breach, Equifax has yet to send an executive to testify before Congress who actually has the ability to examine all the issues with our broken credit reporting system. Committee Democrats requested this minority day hearing and invited the chief executive officers of Equifax, Experian, and TransUnion, which are the three nationwide consumer reporting agencies in this country, as well as a group of senior staff from legal authority to commit the company to future action.

Equifax has badly mishandled virtually every aspect of this breach. They failed to update a known software vulnerability for several weeks. They failed to properly notify law enforcement agencies, as required by many State data breach laws and regulations,

and even in announcing to the public about the breach, failed to provide consumers with the tools they needed to safeguard against identity theft and other harm that could be caused by the unauthorized exposure of their sensitive financial and personally identifiable information for free.

But Equifax isn't the only major credit bureau to have faced a major cyberattack. About 2 years ago, Experian, one of the other major bureaus, also had a breach that exposed millions of T-Mobile customers' information. Yet the head of Experian also declined to come to testify today.

These security breaches at the major credit bureaus are just one of the many problems within the credit reporting industry. That is why I have long called for a complete overhaul of the entire credit reporting system, and I recently introduced H.R. 3755, the Comprehensive Consumer Credit Reporting Reform Act. My bill shifts the burden of removing mistakes from credit reports onto the credit bureaus and furnishers—away from consumers—limits credit checks for employment purposes, and reduces the time period that negative items stay on credit reports, among many other key reforms.

It is clearly time for us to fix the vast problems within the credit reporting sector. There is enormous concern and frustration from consumers across the country about the lack of control they have over how these companies collect, maintain, and sell consumer data.

It is time for us to ensure there are adequate measures to hold these firms accountable for their business practices. And I find it unacceptable that the three major credit bureaus have still failed to take even the most basic steps to protect consumers after this latest massive breach by immediately providing all consumers with free credit freezes.

If executives at the three nationwide consumer reporting agencies are watching this hearing today, I want them to know that the days of their companies being able to operate with impunity are now over. I thank you, and I yield back the balance of my time.

Mr. BUDD. Gentelady yields back.

The Chair now recognizes the gentleman from Michigan, Vice Ranking Member Mr. Kildee, for 1 minute.

Mr. KILDEE. Thank you, Mr. Chairman.

And thank you to the Ranking Member for organizing this important hearing. This breach, the Equifax breach should never have happened. Because of unacceptable security lapses, Equifax exposed the personal information of over 145 million Americans.

For a company whose very business involves the collection of America's most personal financial information, it is almost inconceivable that this major breach occurred. And I know I am, and other members of this committee, are very concerned with potential insider trading by several high-level Equifax executives, and we have requested the SEC (Securities Exchange Commission) to fully investigate these actions.

Even worse than the breach itself, or the potential insider trading, has been how Equifax treated the American public and its customers since this breach was exposed. Weeks passed between the discovery of this breach and when it was disclosed to the public,

yet Equifax was completely unprepared to address the concerns of Americans.

I am grateful that we are having this hearing today to see how we can move forward and make sure this does not happen again and to do what we can to help the over 145 million Americans impacted. Thank you, and I yield back.

Mr. BUDD. Gentleman yields back.

The Ranking Member is recognized for 4 minutes to introduce the panel of witnesses.

Ms. WATERS. Thank you very much, Mr. Chairman.

And welcome to all of our witnesses today. First I would like to introduce Sara Cable. Ms. Cable is an Assistant Attorney General and the Director of Data Privacy and Security in the Consumer Protection Division of the Massachusetts Attorney General's Office as an Adviser to Attorney General Healey and her chief of staff.

Ms. Cable leads the office's data privacy and security enforcement and advocacy efforts. Ms. Cable oversees the office's review of thousands of data security incidents each year and leads several investigations of data security and privacy matters affecting the financial, health care, insurance, legal, and retail sectors.

And then there is Kathleen McGee. Ms. McGee is presently the Chief of the Bureau of Internet and Technology for the Office of the New York State Attorney General. The bureau is responsible for the enforcement of New York's privacy, data security, and consumer protection laws in the online and technology environment, as well as for enforcement of New York's data breach notification laws. The bureau investigates a wide range of issues affecting the tech space, including privacy violations, data security breaches, online safety, native advertising, deception, and fraud.

Then there is Chi Chi Wu. Ms. Wu is a Staff Attorney at National Consumer Law Center (NCLC), where her specialties include fair credit reporting, credit cards, tax-related consumer issues, and medical debt. She frequently serves as a resource for policymakers and the media on consumer credit issues. Ms. Wu is the lead author of the NCLC treatise Fair Credit Reporting Act and has been advocating for a reform of the credit reporting system for over a decade.

And then there is Laura Moy. Ms. Moy is the Deputy Director of the Center on Privacy and Technology at Georgetown Law. She is a public interest advocate who writes and speaks on a number of technology policy issues, including consumer privacy and law enforcement surveillance. Ms. Moy has testified previously before this committee, and we are pleased she is here with us again today.

Mike Litt—last, but certainly not least—Mr. Litt is a national consumer advocate for the U.S. Public Interest Research Group (PIRG) an organization that advocates for the interest of American consumers and stands up against power interests when they push the other way. He is a leading voice on credit freezes and identity theft prevention and has co-authored a number of valuable resources on the topic.

Again, I want to welcome all of our witnesses to today's hearing and thank you for being here today. I yield back the balance of my time.

Mr. BUDD. Gentlady yields back.

Ms. Cable, you are recognized for 3 minutes to give an oral presentation of your testimony.

#### STATEMENT OF SARA CABLE

Ms. CABLE. Thank you.

Good afternoon, Chairman, Ranking Member Waters, distinguished members of the committee. Thank you for inviting me to testify today.

My name is Sara Cable. I am an Assistant Attorney General in the Massachusetts Attorney General's Office and Director of Data Privacy and Security in its Consumer Protection Division.

On September 19th, our office filed the first State civil enforcement action against Equifax. Our goal with our suit is to hold the company accountable for the harm it caused nearly 3 million of our consumers, approximately half of the adult population of our State, harm that, in our view, Equifax could have and should have prevented.

We sued Equifax under our State Consumer Protection Act and our Data Breach and Data Security Laws, which are recognized as among the strongest in the Nation. We allege that this breach was foreseeable and preventable, but that Equifax failed to develop, implement, and maintain reasonable safeguards required by Massachusetts law to protect the sensitive personal data of the consumers it held in its systems, and presumably off which it profited.

Because my time is short, I want to highlight one key point for the committee. While the Equifax breach may be notable for its scope and impact, it is not unique. Our experience strongly suggests to us that businesses large and small are not doing what they need to be doing to protect consumers' information from foreseeable threats.

Over the last 10 years, since the Massachusetts Data Breach Notice Law went into effect, our office has received notice of over 19,000 data breach incidents impacting Massachusetts residents. In 2016 alone, we received notice of over 4,000 data breaches. This is 25 percent more than in 2015 and a nearly tenfold increase from 2008, the first full year that our breach law went into effect.

Now, with this kind of volume, we can't possibly investigate every single breach. And I think it is worth noting that just because a company is breached does not necessarily mean that it did anything wrong or that it failed to have reasonable safeguards in place. But for the ones into which we take a closer look, it suggests to us that many of these breaches could have been prevented through reasonable, and indeed basic, security safeguards.

To this day, we continue to see breaches impacting entities in every sector that result from the failure to employ basic security safeguards in compliance with Mass law. And just some of these are companies that don't even have a written information security program, much less follow the one that they have; companies that cut corners by using outdated and unsupported software; or companies hoarding vast amounts of sensitive consumer data in their network without a present or contemplated business need and leaving it unsecured.

Now, to be sure, there are entities that do it right, but we are seeing far too often that entities are not treating consumers' infor-



mation like the valuable asset it is. And that is even with the constant drumming of headlines about the risks of data breach incidents.

And I will conclude to note that, in the case of Equifax, which was subject to both State and Federal law, even that law as it exists today was not enough to prevent this breach. And I would submit that any law that is proposed that is weaker than the law that we currently have today is worse than doing nothing for consumers.

Thank you very much.

[The prepared statement of Ms. Cable can be found on page 28 of the Appendix.]

Mr. BUDD. Thank you.

Ms. McGee, you are now recognized for 3 minutes to give an oral presentation of your testimony.

#### STATEMENT OF KATHLEEN MCGEE

Ms. MCGEE. Thank you, Mr. Chairman, Madam Ranking Member, and other distinguished committee members.

I am Kathleen McGee, Chief of the Bureau of Internet and Technology at the New York State Office of the Attorney General, Eric T. Schneiderman. Thanks for the opportunity to testify today.

After learning about the Equifax breach, our office immediately launched an investigation. And while I cannot share the details of that ongoing investigation, suffice it to say, we are getting to the bottom of the Equifax breach and are working to ensure credit bureaus protect the sensitive consumer data that they hold.

States have had a central role in protecting consumers and their data for nearly 2 decades, as my written statements detail more fully. But in these remarks, I would like to make a few points regarding any Federal legislation.

First, law must keep pace with the ever increasing rate of technological change. States have proven the ability to act quickly in that regard, and Congress should not limit States' ability to innovate in this area.

Second, when it comes to enforcement, States occupy a leading role and must continue to do so. States together play a big role after major breaches like Target or Equifax, but less well-known are actions taken in response to smaller breaches that occur in the hundreds each year in New York and other States. Even under the best of circumstances, it is unlikely a Federal agency would be as responsive as the States to breaches involving local business and relatively small numbers of local consumers.

These breaches may be smaller, but the victims are no less in need of law enforcement protection. Smaller breaches are the rule, not the exception.

I respectfully urge this committee to ensure that any data security or breach legislation meets the following requirements, which we consider vital to protecting consumer data. First, any bill should not preempt State law. Indeed, it should expressly set a floor, not a ceiling on data security and breach response standards.

Second, as with many other Federal consumer protection laws, Federal data security requirements must be enforceable by States,

as well. And any Federal penalties must be recoverable by the States, as well.

Third, if preemption is contemplated, the language must be drawn very carefully to avoid unintended consequences. Broad preemption language might be interpreted to set aside laws that concern personal privacy or computer crimes, causing serious public harm.

In the meantime, as this body considers legislation and States continue to innovate, our office will continue to enforce data security protections on behalf of New Yorkers and to work with New York State's lawmakers to update our own protections. We very much appreciate your committee's efforts. And I thank you for your time today.

[The prepared statement of Ms. McGee can be found on page 99 of the Appendix.]

Mr. BUDD. Thank you.

Ms. Wu, you are now recognized for 3 minutes to give an oral presentation of your testimony.

#### STATEMENT OF CHI CHI WU

Ms. WU. Mr. Chairman, Ranking Member Waters, and members of this committee, thank you for inviting me to testify today.

I am testifying on behalf of the low-income clients of the National Consumer Law Center. NCLC has long advocated for the need to reform the U.S. credit reporting system. We have testified many times before Congress about the unacceptable error levels in credit reports—one in five consumers, with one in 20 having very serious errors—and the Kafkaesque methods that these companies use to handle disputes, creating an automated version of voicemail hell and always siding with the creditor or debt collector that provided the wrong information.

These inaccuracies, the barriers consumers face in trying to fix errors, and the Equifax data breach all stem from the same origin: A corporate culture of impunity and arrogance, which you can also see by the fact that all three credit bureau CEOs failed to show up today.

By now, you have probably heard the refrain that American consumers are not the customer, but rather the commodity of credit reporting agencies. We can't vote with our feet; we are captives. As a result, the credit reporting agencies get away with all sorts of abuses, cutting corners in personnel and systems, and failing to invest in doing things right.

A March 2017 report from the Consumer Financial Protection Bureau (CFPB) documented these issues, prompting Director Cordray to remark, "We were surprised to find that their quality control systems were either rudimentary or virtually nonexistent."

Now, a data company that underinvests in quality control for accuracy and compliance is likely to be the same company that will underinvest in information security. It all stems from the same attitude, "Let's just see how much we can cut costs." And Equifax is not alone. We think Experian and TransUnion suffer from similar cultures.

So what is to be done? One suggestion has been to give authority to the Consumer Bureau under the Gramm-Leach-Bliley Act to supervise for data security. And we completely agree with that. But just as critically, we believe Congress should enact wider reforms of the credit reporting industry.

That is why we strongly support H.R. 3755 and we thank Ranking Member Waters for introducing it. H.R. 3755 would vastly improve the broken credit reporting system, increase accuracy, and help victims of abusive lending and overly punitive negative reporting practices.

Another reform we need are free security freezes. Victims of Equifax's negligence shouldn't have to pay to protect themselves from the threat of ID theft. Equifax and TransUnion have offered free credit locks, but a lock isn't the same as a freeze. A lock isn't required by law so there is limited recourse if something goes wrong. Plus, Equifax and TransUnion could stop offering free locks at any moment. Also, TransUnion's lock requires consumers to agree to forced arbitration and receive targeted advertising.

And by the way, last night's Senate vote nullifying the bureau's arbitration rule is only going to increase the culture of arrogance and impunity. And Experian isn't even offering free locks or free freezes.

Thank you for the opportunity to testify and I look forward to your questions.

[The prepared statement of Ms. Wu can be found on page 124 of the Appendix.]

Mr. BUDD. Thank you.

Ms. Moy, you are now recognized for 3 minutes to give an oral presentation of your testimony.

#### **STATEMENT OF LAURA MOY**

Ms. MOY. Good afternoon, Mr. Chairman, Ranking Member Waters, and the members of the committee. Thank you so much for inviting me to testify.

Consumers are frustrated, as I think many members of this committee are. We lack control over what happens with data about us. We lack control over who has access to information that we should be able to control: Information about our finances, health, and families; information about things we do in the supposed privacy of our own homes; information about where we go, who we speak to, and what we think; information that can be used to steal our identities, ruining our finances, and maybe even our employment.

Congress cannot lead from behind in protecting consumers. A breach of sensitive data is a bell that cannot be un-rung. Consumers need better control and protections, closer regulatory oversight, stronger enforcement, and greater incentives for companies to do the absolute best they can to protect our information.

And companies can do much better. The massive Equifax breach happened over the course of months because the company failed to patch a critical system vulnerability about which it had ample notice and failed to detect the breach once it was underway.

I urge this committee to give full consideration to the policy recommendations advanced by my fellow witnesses today. In my limited time, I would like to offer a few key points.

First, I agree with my co-panelists that preemption of State law is not the answer. States are the engines of reform, and State laws on data security, medical identity theft, and protection of biometric data are some examples of some of the critical innovations happening at the State level.

Federal legislation in this area should set a floor, not a ceiling, to allow for critically important State laws, especially those on data security and breach notification. But Federal legislation is needed. Federal legislation should avoid a so-called harm trigger that limits protection to potential financial harm.

The breach of personal information is a serious harm in its own right. And consumers may suffer serious emotional or even physical harms or misuses of their personal information. Harm is not limited to financial harm alone.

Federal legislation must also be sufficiently flexible so it covers information that is captured by emerging technology. We can't always forecast the next big threat, but unfortunately, we know that there will be one. Whether by continuing to allow States to increase protections on their own or establishing agency rulemaking authority to define covered information moving forward, Federal legislation must provide flexibility to meet new threats.

Federal legislation should also include robust enforcement authority for both Federal and State regulators. Given the thousands of data breaches, and you just heard some of those numbers, in the thousands of data breaches reported each year, Federal authorities alone cannot protect consumers. State attorneys general and other State regulators must play a critical role.

Thank you, and I look forward to your questions.

[The prepared statement of Ms. Moy can be found on page 103 of the Appendix.]

Mr. BUDD. Thank you.

Mr. Litt, you are now recognized for 3 minutes to give an oral presentation of your testimony.

#### **STATEMENT OF MIKE LITT**

Mr. LITT. Thank you, Mr. Chairman, Ranking Member—as a consumer advocate for U.S. PIRG, I appreciate the opportunity to discuss next steps after the Equifax breach. Equifax still has not provided or even clearly explained what is needed to fully protect consumers.

Once your information has been stolen, there is only one kind of ID theft that can be stopped before it happens. That is where somebody opens a credit account in your name. The way to prevent that is by blocking access to your credit reports with all three credit bureaus.

It is beyond time for all consumers to have the right by law to control access to their credit reports with free credit freezes.

In my written testimony, I explained how Equifax's TrustedID Premier product fails to fully protect consumers. I also highlight concerns with its forthcoming lifetime lock. Locks and freezes ap-

pear to function similarly in that they block access to your credit report. The bottom line is freezes are better because they are a right by law and not conditional on terms set by the credit bureaus.

Also, creditors run credit checks with any one or a combination of credit bureaus, so it is important that you block access to your credit reports at all three bureaus. Getting a lock or a freeze at just one but not the others is basically like locking your front door, but leaving your garage and back doors wide open.

All 50 States and D.C. have their own laws governing fees for freezes, temporary lifts, and permanent removals. There are approximately 158 million consumers in 42 States that must pay a fee between \$3 to \$10 per bureau. We did not give the credit bureaus permission to collect our information or sell it or, in the case of Equifax, to lose it. So why do we have to pay to control access to our reports?

The PIRG has helped pass the first State freeze laws. Now we support Federal legislation that would set free freezes for all Americans as the floor. We also support legislation that would require freezes to be placed within 15 minutes of online and phone requests, as is the law in 10 States and D.C. States should be allowed to find even more ways of giving consumers control over access to their own reports. Federal legislation should not preempt or replace existing stronger State laws for privacy, breach notification, or data security, either.

We also strongly support H.R. 3755, introduced by Ranking Member Waters. While the transfer of Fair Credit Reporting Act responsibilities to the consumer bureau has jumpstarted the compliance efforts of the big three credit bureaus, this bill will give required improvements.

Thank you for your attention and for the opportunity to present my testimony.

[The prepared statement of Mr. Litt can be found on page 90 of the Appendix.]

Mr. BUDD. Thank you.

The Chair now recognizes the distinguished Ranking Member, Ms. Waters, for 5 minutes.

Ms. WATERS. Thank you very much, Mr. Chairman.

It is unfortunate that the three CEOs for the major credit reporting agencies rejected the opportunity to discuss their business model and what actions Congress should consider in the wake of the Equifax data breach to better oversee the use of consumer data.

So let me ask each of the panelists: Do consumers have sufficient control over the existing use of, and commercialization of, their data collected, maintained, and compiled by the largest consumer reporting agencies and other businesses? Let me just go down the line, start with Ms. Cable. Do they?

Ms. CABLE. Sure, thanks for the question. I would submit, no, they don't.

Ms. MCGEE. I would submit that was a rhetorical question. No, they don't.

Ms. WATERS. Ms. Wu?

Ms. WU. Absolutely not. They need more control and protection.

Ms. WATERS. Ms. Moy?

Ms. MOY. Absolutely not. And they are frustrated and asking for more.

Ms. WATERS. Mr. Litt?

Mr. LITT. Absolutely not. They need that control.

Ms. WATERS. OK. I would like to go back to each of you and ask you if you could briefly mention maybe one action Congress should take with respect to the oversight of consumer reporting agencies, to empower consumers to have better control of their personal information? Just one thing, each of you, starting with Ms. Cable.

Ms. CABLE. I could say under State law in Massachusetts, our legislators have proposed a bill that would require entities seeking a credit report to get the consumer's written consent before they do so.

Ms. WATERS. All right.

Ms. MCGEE. I think New York's big focus here is on transparency and acknowledgment that the consumer understands what data is being collected about her and how it is being used.

Ms. WATERS. Thank you.

Ms. Wu?

Ms. WU. We would advocate for free credit freezes or even freezes by default, also a strong Consumer Financial Protection Bureau and the ability of the bureau to supervise for data security.

Ms. WATERS. Ms. Moy?

Ms. MOY. I think that many companies know what they ought to be doing on data security and they are not doing it. And I think that we need stronger enforcement authority accompanied by civil penalties.

Ms. WATERS. OK. Mr. Litt?

Mr. LITT. It is time for consumers across the entire country to have the right to control access to their credit reports with free credit freezes.

Ms. WATERS. Thank you so very much.

I think Ms. Wu mentioned that you are familiar with the bill that I introduced. And we tried to address those issues, each of those issues that you have identified.

I have one other that concerns me greatly, and that is the use of this data, individuals' data in employment efforts that are being made. An individual applies for a job and the job requires that they check their credit, that their credit be checked. Do you think that credit information should be used in employment efforts?

Ms. Wu?

Ms. WU. I do not think credit reports should be used in employment, except for very, very, very narrow circumstances. I absolutely support the provision in H.R. 3755 to severely restrict the use of credit reports in employment. It is bizarre. Somebody loses their job, they can't pay their bills, and their inability to pay their bills means they can't get another job. And credit has nothing to do with your ability to perform a job.

Ms. WATERS. Thank you.

And let me ask Ms. McGee. We have tried to reduce the time that negative information stays on your credit report. What do you think about that?

Ms. MCGEE. We support that. We supported that provision in the National Consumer Assistance Plan that we agreed upon with the

three credit reporting agencies. And we see that H.R. 3755 provides some very robust protections with respect to consumers. We support that.

Ms. WATERS. Thank you.

Ms. Moy, what else can we do to ensure that consumers have access to their credit information? How often should they be able to get it? How should the bureaus respond to the request for information that they have collected on you?

Ms. MOY. So I agree with what others have said, that freezes ought to be something that consumers can have on an ongoing basis and for free. I also think that while one credit report annually is a place to start, I think that—particularly if credit reports are being accessed by folks, by entities without the consent of the consumer, and particularly if they are being accessed for purposes such as employment—then consumers ought have access to their credit report on an ongoing basis, not just a view into it once a year.

Ms. WATERS. Thank you.

Mr. Litt, many people are wondering what they can do to protect themselves who are victims of the breaches that have taken place. What about credit freezes? Should they be charged? And if they are charged, how long should that charge continue, like with Equifax?

Mr. LITT. Yes, consumers should not be charged to have access to their own credit reports or to control access to their own credit reports, which is really the only way to protect yourself from new account identity fraud, which is the only kind of identity theft that can actually be prevented once your information is out there. Unfortunately, there are far too many Americans who have to pay a fee between \$3 to \$10 per bureau, and that should stop.

Ms. WATERS. Thank you.

I yield back the balance of my time.

Mr. BUDD. Chair now recognizes the gentlelady from New York, Mrs. Maloney, for 5 minutes.

Mrs. MALONEY. Thank you. I want to thank the Ranking Member for looking out for consumers and calling this important Oversight Committee.

I would first like to ask Ms. Wu, as you know, one of the reasons why the Equifax breach was so bad was that the information that was stolen included the Social Security numbers and the date of birth for over 145 million people. That is half the population of this country.

And both of these materials are critical pieces of identification that cannot be changed. And this is a huge problem for 145 million people.

Now, some people have suggested that we should move away from using the Social Security numbers as a key piece of identifying information and start using unique ID numbers that are more easily changeable. Do you think that would be helpful? And if so, what do you think should be in charge of coming up with new ID numbers that would replace Social Security numbers? And that is the question for Ms. Wu.

Ms. WU. Thank you for the question Congresswoman Maloney. The fundamental issue with the case of the Social Security Number is it is used as a verifier, not as an identifier, or both as a verifier

and an identifier. It is like using your e-mail address as your password. That number shouldn't be serving two roles.

You do need a number, some sort of identifier number for credit reports—just make sure you've got the right person. And in fact, what we have criticized credit reporting agencies for years was using partial Social Security numbers to match people because that results in things like mixing two people's credit files up.

But you do need better ways to verify that someone is who they say they are. And, I suggest that an entity like the Consumer Bureau is a good one to start figuring out those issues.

Mrs. MALONEY. OK, thank you.

Now, as you know, Equifax was covered by the Fair Trade Commission Safeguards Rule, and this is intended to ensure the security and confidentiality of this sensitive information. Now, I happen to think that Safeguards Rule is one of the strongest data security rules out there.

It is the same rule that banks and credit unions are subject to and has largely been successful since it was first established by this body in 2002. And I think Equifax blatantly violated the Safeguards Rule by not having an information security system in place that can identify reasonably foreseeable risks.

And in this case, they were notified. They were notified by the Homeland Security Department that there was this type of weakness in the system. The other two groups caught it. They didn't even bother to correct it.

So I want to ask you, if the Safeguards Rule had been properly enforced and implemented by the FTC, then the Equifax hacks shouldn't have happened in the first place. But it is also possible that we need to look at updating the Safeguards Rule in light of the breach.

So, Ms. Moy, and I would like to follow it with Mr. Litt, what are your thoughts on this? Do you think we need to update the Safeguards Rule or do you think we just need to ensure that the rule is properly enforced? Obviously, Equifax did not enforce this rule even when they were notified that this type of breach would happen.

So, first, Ms. Moy, and then I would like Mr. Litt to answer, too.

Ms. MOY. Thank you. That is an excellent question. And, as I said before, I think a lot of times companies know what they need to do and they are just not doing it. And it seems that that was in fact a case with the Equifax breach. As you mentioned, they were notified of the critical vulnerability in Apache Struts back in March and failed to, by DHS.

But I will just say I do think that it is time to take a look, at least, at updating the Safeguards Rule. For example, it could explicitly mention encryption.

Mrs. MALONEY. Yes or no, because my time is running out, Mr. Litt, should we update the Safeguards Rule?

Mr. LITT. Yes, we should finish updating the Safeguards Rule.

Mr. MALONEY. OK. Now, I would also like to ask you, in light of Equifax's decision to wait a full 6 weeks to notify the public of the breach, do you think that part of the problem is that there is no explicit data breach notification provision or requirement in the Gramm-Leach-Bliley Act?



Mr. LITT. We believe that any kind of Federal legislation would need to set a floor and not preempt stronger existing State laws.

Mrs. MALONEY. OK. Ms. Moy, what do you think?

Ms. MOY. So I think many consumers do feel at the point where they get notification, it is too late. That said, I do think that folks ought to know that their information was breached.

Mrs. MALONEY. My time is expired. Thank you very much.

Mr. BUDD. Thank you.

The Chair now recognizes the gentleman from California, Mr. Sherman, for 5 minutes.

Mr. SHERMAN. Mr. Chairman, we have had a tradition in this committee room of every Republican member putting the national debt clock up while they had their time. Earlier today, that seems to have been suspended, and the only member to put up the national debt clock during hearings we had earlier today was myself.

Are you familiar as to why this change was made? Does it have anything to do with a budget resolution we are voting on tomorrow that will add a couple of trillion dollars to that debt clock?

I yield to the Chairman.

Mr. BUDD. I yield without comment back to the gentleman from California.

Mr. SHERMAN. The gentleman's response is instructive. In an effort to stay true to Chairman Hensarling's commitment to a balanced budget, I will continue to have the national debt clock up during my 5 minutes. Not that I don't think the graphics presented by our Ranking Member aren't excellent, I know that they will be up during much of today's hearing.

I will point out I have added two things that I would commend to Chairman Hensarling. One is to add to the fact that the Republican tax cut will add \$150 billion to \$200 billion. And this committee has played a role in pressuring the Fed to abandon quantitative easing, and that will add another \$80 billion to \$100 billion a year to our national debt. So while the flame of fiscal responsibility may have been blown out of one side of the room, the flame continues to flicker on this side.

Mr. Litt, people are talking about locking versus freezing. And you pointed out that if you are going to do either, you have to do it with all three credit rating agencies. Equifax says they will do one for free. Will they pay the fee, though, to the other two credit rating agencies to lock or freeze your credit? Or is that on the consumer?

Mr. LITT. Disappointingly, they have not said whether they will do that or not, and they are calling on TransUnion and Experian to offer free locks. And so they are not paying for that.

Mr. SHERMAN. OK, so they are the ones that screwed up.

Mr. LITT. Exactly.

Mr. SHERMAN. So their competitors should pay the cost. My God, it is as if my locksmith lost my key and he will provide a new lock to my front door, and then he calls upon competing locksmiths to provide me with a replacement for my back and side doors. That is amazing.

I will ask the representative for the New York Attorney General's Office, is there an effort to hold Equifax accountable and sue them for whatever consumers have to pay, or better yet, to estab-

lish a fund that would fund consumers locking or freezing their credit with the other two agencies?

Ms. MCGEE. As I mentioned earlier, we are pursuing an investigation, so I am not going to comment on relief that we might seek, except to say that we are seeking full relief for New York consumers as Massachusetts is seeking full relief for their consumers. And we are looking at the full system. We have publicly called in Equifax and their competitors, as well, to understand the system better and to see whether or not there could be structural changes.

Mr. SHERMAN. Thank you. So as soon as Mr. Hensarling will cosponsor the bill, I will introduce legislation to say that if you have a data breach where you have even advised people that they need to buy three locks, that you have to provide one of the locks for free and pay for the other two.

To say that Equifax should call upon its competitors to do this for free, perhaps there could be some reduced cost, but as things stand now, though, Mr. Litt, if I want to implement Equifax's suggestions, I go to Equifax and I freeze or lock my file, and then I pay money out of my own pocket to freeze or lock at the other two agencies. Is that correct?

Mr. LITT. That is right.

Mr. SHERMAN. I yield back.

Mr. BUDD. Chair now recognizes the gentleman from New York, Mr. Meeks, for 5 minutes.

Mr. MEEKS. Thank you, Mr. Chairman.

You know, indeed, this is a sad day, I think, for consumers. Let me start out that way. I have to start out by saying, first, I am disappointed but not surprised at all, even though it is not directly related to this hearing, that my Republican colleagues in the Senate along with the assistance of the Vice President of the United States and the White House decided to roll back consumers' access to the courts in favor of the most powerful players in Washington, D.C. Bad day for consumers.

Instead of protecting options for consumers, i.e., consumers who are merely seeking a recourse for the wrongs done to them, my Republican colleagues have opted to limit choice and force consumers into unfair arbitration agreements that stack the cards against them.

I am also concerned that I think it is unprecedented that you have a person who is serving on an acting basis for the OCC decided to insert himself in this debate, and I believe placed inappropriate political pressure on what is supposed to be an independent CFPB. And I just have to take this opportunity to remind people that an independent CFPB was not there prior to the 2008 crisis. In fact, there was no agency focused primarily on the consumer.

And sure, we had banking regulators responsible for ensuring institutions operated with prudence and in a proper way. However, we had no single player at bat for the consumer. So we created this independent Consumer Financial Protection Bureau that this Administration and my Republican colleagues continue to undercut and undermine with little regard for the consumer and the underdog.

So, regarding today's hearing, I am further disappointed that Equifax refused to appear before this committee again. And I be-

lieve that avoiding responsibility is a proven failed strategy in Washington, D.C.

As we saw with, and has happened in this committee before, when the Enron executive that pled the Fifth before Congress, and the Wells Fargo's past CEO who failed to acknowledge his poor oversight. And then we had Equifax's prior CEO come in here, he said is no longer with Equifax and so the individuals who are now in charge of Equifax, they, in fact, have not been before this committee yet. It was bad advice then and it is bad advice now.

Furthermore, I hope that Equifax can correct the Congressional Record, because when this former employee was before this body at our last hearing, he suggested to me that Equifax had a breach response plan that was tested prior to its May incident. A recent Wall Street Journal report alleges just the opposite.

Therefore, I am very concerned that Equifax's former CEO potentially made misstatements before this committee. I hope he is not getting in the habit of the 45th President, who continues to make misstatements whenever he speaks.

The Wall Street Journal reported the following: Equifax was ill-prepared to face the increasing frequency of data breaches and that a review of the company found, and I quote, no evidence of regular cybersecurity audits, or an emergency plan to respond to an intrusion. So I sent a letter to Equifax to correct the Congressional Record. I have yet to hear back from them.

Now, I am going to ask my friend—I know that we have Kathleen McGee here who is from my friend Attorney General Schneiderman's office. Let me just ask you, real quickly, in what ways can States help get institutions to a place where they are better prepared for the next breach? What are you doing in New York? And what can we utilize nationally to help make sure this never happens again?

Ms. MCGEE. Thank you. Across this country, 48 States and territories, all the territories, have data security laws in place. We are the incubators and the innovators for the frontlines for innovation and data technology. We are the gatekeepers. We innovate and protect consumers on the ground.

We should not be superseded or preempted by a Federal law. And we would encourage that this body consider establishing a stricter floor, not a ceiling, if it considers passing a national standard.

Look to the States for the innovation. New York has good suggestions, Massachusetts. California was an innovator passing the initial law back in 2002. So we would suggest you look to the States first. Thank you.

Mr. BUDD. Thank you.

The gentleman from California is well aware, the debt clock is traditionally used only at full committee hearings. And my Democratic colleagues previously requested we not display it during their questioning time. Also, members are reminded not to engage in personalities.

The Chair now recognizes the gentleman from Georgia, Mr. Scott, for 5 minutes.

Mr. SCOTT. Well, thank you very much, Mr. Chairman.

First of all, I wanted to commend our Ranking Member, Ms. Waters, for putting this hearing together.

And then, second, I am the Georgia Congressman representing Equifax. And I can't tell you how disappointed, I can't tell you how insulting, I can't tell you how just downright rabid that they are making me as a Georgia Congressman.

Now, with this terrible breach, impacting 145 million people—and first, they send up here to speak to us the former CEO. How, I ask these panelists, do you think—and the American people—that we can even begin to fix this problem if these bone-headed executives and current CEO will refuse to come before Congress and to answer questions?

How can they expect to get a seat at the table? How can we respond to the American people? Some of these American people don't even know what Equifax does or these credit agencies. Their lives are impacted in a very negative way.

And yet they will refuse to come before Congress. Now, they may be thinking that they are sticking it to Members of Congress, but when you violate Members of Congress, when you insult Members of Congress, when you disrespect Members of Congress, you are insulting and disrespecting the American people. We speak for them. And for them to do this is a dastardly deed.

And I hope, Ms. Waters, that you will pursue my request that we had yesterday evening to ask for a subpoena. That will get their lazy asses up here and respond to the American people.

Now, I apologize for anybody that feels I have offended you with that, but I meant it. That is what they are. And until they are sitting in that chair, we have to hold Equifax accountable.

Let me tell you what they did. Do you know what they did? In March, they brought evidence of the leak. They also brought a way to fix the leak, with a patch, and they refused. The CEO at that time, Mr. Smith, said that he found out on July 1st.

And then, the most dastardly deed of all that they did was they went 24 hours later and sold \$2 million in stock, and not just anybody, their three top executives, led by their chief financial officer. And you mean to tell me that nobody is looking at this as insider trading?

This is one of the most despicable, shameful acts of financial mismanagement in the history of these United States. And for them not to come before this Congress and answer these questions, the people who will run the company, is a total disrespect. And not only that, it is highly un-American. And it is not something that I will accept.

Ms. Wu, I want to ask you this. Tell me, the American people need to know, will they be having to look beyond their shoulders, looking around corners worried for the rest of their lives because they don't know who has their Social Security, they don't know who has their birth—these are vital pieces of information. Is that what we have to look forward to? Could you please answer that?

Ms. WU. Unfortunately, the answer is yes. We will all be looking over our shoulders for the rest of our lives.

Mr. SCOTT. Thank you.

Mr. BUDD. Gentleman's time has expired.

Chair now recognizes the gentleman from Texas, Mr. Green, for 5 minutes.

Mr. GREEN. Thank you, Mr. Chairman.

I especially want to thank the Ranking Member for her energy and effort to cause this hearing to take place.

Equifax is in a unique position. They collect information on consumers without consent. They don't have to have your consent to collect your information. Once they collect the information, they seem to think that they can handle it with impunity. If there is negligence or if there is some reason for a security breach that might cause litigation in ordinary circumstances, Equifax seems to think that arbitration is the methodology by which a dispute should be resolved.

It causes me great concern to know that Equifax and many other companies, especially banks, are being aided and abetted by Congress, because Congress, yesterday, the Senate more specifically, decided to eliminate the consumer protection rule that would allow consumers to litigate as opposed to go to arbitration.

This is an unbelievable circumstance. And I am interested in comments from members of the panel on your position as it relates to arbitration, especially with a company that collects information without your permission.

Let's start with our very first panelist, if you would please, ma'am.

Ms. CABLE. Thank you for question. I think it is safe to say our office's position is that we are disappointed in the developments of yesterday. I think it is a big step back for consumers. I think the unfairness in the Equifax matter is patently obvious to anyone.

And it is one of the big reasons why, as a State attorney general, we are working so hard to hold Equifax accountable for this. And to circle back on how we hold Equifax accountable here, I think money talks. Without getting to the specifics of what we may or may not request in litigation, our Consumer Protection Act authorizes us to ask the court to award us up to \$5,000 per violation. There are at least 3 million violations in Massachusetts.

And so we think the State attorney generals are uniquely positioned and, in light of yesterday's development, may be a very few of the entities still positioned to hold Equifax accountable in the court of law.

Mr. GREEN. Ms. Cable, if you would please, I detected a moment of candor. You said money talks. Kindly explain, please.

Ms. CABLE. I think a way to get the attention of a company like Equifax is to—how do I say this—require them to internalize the costs of this breach that they seem so eager to externalize onto the American public.

Mr. GREEN. And how does one go about this, please?

Ms. CABLE. In our litigation under State consumer protection law, we can seek civil penalties, as I mentioned, up to \$5,000 per violation. We are also authorized to seek consumer restitution for ascertainable losses that consumers suffer.

We are also authorized under our law to have the court impose permanent injunctive relief to improve security procedures and other appropriate relief to make consumers whole. Certainly, all of those are on the table in our litigation.

Mr. GREEN. Ms. Wu, please. Yes.

Ms. WU. So, absolutely, consumers were the losers in the vote last night. And any Republican who voted for getting rid of the arbitration rule, and yet criticized Equifax, was a hypocrite, because Equifax will greatly benefit from what happened last night. Not only because they will be able to immunize themselves from liability over things like credit monitoring products, but because they can actually put in arbitration agreements—for these locks, for example, that they are offering, so-called, for free—that you have to agree to arbitration. And they can put things in those arbitration agreements like “You will never sue us under the Fair Credit Reporting Act, no matter how badly we mess up your credit report.” So the American people are definitely the losers.

Mr. GREEN. Mr. Litt, please.

Mr. LITT. There were already concerns with locks, because TransUnion and Experian require consumers to give up their rights to a day in court. So last night’s vote, unfortunately, makes things even more problematic.

Mr. GREEN. Thank you very much. I yield back the balance of my time.

Mr. ROTHFUS [presiding]. Gentleman yields back.

The Chair recognizes the gentleman from Michigan, Mr. Kildee, for 5 minutes.

Mr. KILDEE. Thank you, Mr. Chairman, and again to the Ranking Member, thank you for arranging this hearing.

I am really grateful for the panel for being here. This has been really helpful.

Like probably all of my colleagues, I received a lot of complaints about this breach, and particularly about the way customers were treated by Equifax as they tried to, somehow, figure this out and manage it.

So I want to tell the story of an individual from my district. His name is Jim. He is from Linden, Michigan. It is a small town outside of my hometown of Flint. He is a grandfather. He has got five grandchildren. He is a retired banker. He spent his whole career working with credit reporting agencies. He understands exactly how they operate.

When he heard about this breach, Jim went to the Equifax website to see if his information had been released, had been stolen, in effect, which it had been. So he, like many, decided he would freeze his credit as a precautionary measure. So in navigating through their website, he wound up not on the page to freeze his credit, but on the page where Equifax offered, for purchase, its product to protect his identity online. I am sure you understand the irony in landing on that page.

Realizing the error, Jim got on the phone. He called Equifax. He wanted to correct the problem. It took him over an hour on the phone with two different individuals, two different call centers, finally to resolve that issue.

He was also to freeze his wife’s credit, but Equifax charged him \$20 to do so. So he reached out to my office, wanted to make a consumer complaint regarding Equifax. We were able to intervene, get his money refunded. But his biggest complaint was that Equifax

made it so hard for him to deal with an issue that was not his fault and, in fact, was their fault.

This guy is a retired banker. He is tech savvy. He understands customer service; he understands how to navigate a website. He couldn't do it without our help. Not everybody can do that. Not everybody has the presence of mind to call their Member of Congress. And Lord knows, there is no way we could deal with 145 million of these complaints.

So my concern is, what happens to those folks who don't know who to call, who don't know where to go? How do they protect themselves? And so I guess I would ask just for any of the panelists who might want to offer, what do we tell our constituents? How do they protect themselves from something like this?

I mean, what happened with Jim, who knows what the other consequences might be, but the frustration he had—and without our help he would be paying them to fix a problem that they created, let alone the potential of economic ruin that he could have faced as a result of this data being lost and being essentially stolen. What do we tell our constituents? How they protect themselves?

Ms. WU. So, thank you for the question and the story, Congressman Kildee. Unfortunately your constituent is not alone. We have heard of many other stories where consumers had trouble getting freezes and end up actually getting not only a lock product, but a paid lock product. They ended up having to pay for it and of course agree to arbitration, which is now going to prevent them from bringing lawsuits.

It is a terrible situation. All I can say is that they should try to keep working on getting those freezes. If they can't get them, they should complain not only to their Member of Congress and their attorney general's office, but to the Consumer Financial Protection Bureau, which has sometimes had success in dealing with these complaints and getting people's money back.

But that points to the fact we need a strong Consumer Bureau. If we don't have a strong Consumer Bureau, even the little bit of progress we have made in terms of improving accuracy and dispute handling, because the Consumer Bureau can supervise these folks and get into their systems, is going to be lost.

And this is the culture of impunity I am telling you about that I said. You know, this is not just an accident. They deliberately pushed people toward their locks and their paid products when people try to find the freezes.

Mr. KILDEE. Thank you.

Mr. LITT. If I may, a default freeze would actually take care of people if they didn't know that they had to opt in for one. But there should be no barriers, including costs. So, at the very least, freezes should be free to place, as well as to lift.

Ms. MOY. You make the point that the consumers who will lose out the most from a breach like this are those who lack the resources in time or in money to figure out how to protect themselves, and that is a problem that absolutely must be addressed.

Mr. KILDEE. Thank you. My time is expired. I thank the panel, again, and I thank the Ranking Member for arranging this hearing. It is very important. Thank you.

Mr. ROTHFUS. Gentleman's time is expired.

The Chair recognizes the gentleman from Nevada, Mr. Kihuen, for 5 minutes.

Mr. KIHUEN. Thank you, Mr. Chairman, and thank you, Madam Ranking Member, for organizing this hearing, and thank you to all of you for being here and for your testimony.

Mr. LITT. I have a question, and maybe for the rest of panelists as well. Given that half of the population of the U.S. had their Social Security numbers exposed as part of this recent breach, do you find it troubling that such numbers are still being used by Equifax to authenticate consumers requesting freezes, copies of credit reports, and other products and services offered by the consumer reporting agencies?

Mr. LITT. Yes, it is troubling. While the other authentication questions do serve as added security, Social Security numbers were never meant to be used as identifiers to begin with. And so this also raises the question for looking into transition into a new system.

Mr. KIHUEN. What would a new system look like, in your opinion?

Mr. LITT. Well, we would look at things like two-factor authentication as a place to start, and then I think that we are encouraged and hopeful that Congress would look into ways to transition, as well.

Mr. KIHUEN. Thank you. Anybody else want to answer?

Ms. WU. Thank you for the question, Congressman. As I said earlier, the problem is the use of the Social Security number as the verifier to say that you are who you are. You do need some sort of identification number, and whether it is a Social Security number, or something else, you need a unique item to distinguish between consumers.

The former CEO of Equifax, his name is Richard Smith, and you need to be able to figure out which Richard Smith you are dealing with. The problem is, you are also using the Social Security number as the verifier. So, you input that number and then the system tells me, OK, you are the real Richard Smith. And that is the problem. We need other ways of verifying someone's identity.

Mr. KIHUEN. Thank you.

And I have a follow up on that, Ms. Wu. In your testimony, you described this breach as one of the worst, if not the worst, breaches in American history. Apart from the total number of consumers impacted, what else makes this the worst in American history?

Ms. WU. Well, the reason why this breach is probably one of the worst in American history is because of the type of information that is stolen, because it was Social Security numbers and dates of birth, and in some cases, driver's licenses. This is the crown jewel of information that can be used for ID theft.

Other breaches involved your e-mail and password. Well, you can change your e-mail address. You can change your password. Your credit card number, you know, Target involved a lot of credit card numbers. You can get a new credit card number.

It is almost impossible to change your Social Security number. It is very hard. And you can't change your date of birth. So this is going to haunt us forever. This is going to increase the risk of iden-



tity theft for half the American population for the rest of their lives. And that is what makes it so terrible.

Mr. KIHUEN. Thank you. I think you answered my other question that, how long are consumers likely to be at risk? So you were talking about for the rest of their life. So half of the American population who has been impacted by this is now at risk for the rest of their life because of this breach?

Ms. WU. Yes, that is right. And the best we can do is try to mitigate it by telling people to put freezes on their credit reports. And that is why, at least those freezes should be free. And I agree with Mr. Litt, they should be by default. That would help a lot to prevent identity theft.

Mr. KIHUEN. Thank you.

And, Ms. Cable, I do have a very quick question. Immediately following the announcement of the breach, Massachusetts launched an investigation and filed a lawsuit against the company. While I understand that you cannot comment on the status of the case, as the matter is still ongoing, can you provide a high-level overview of allegations your office is making in the privacy and data security and privacy protections that Massachusetts residents are entitled to under the law, State law?

Ms. CABLE. Absolutely, Congressman. So the facts underlying our complaint are the facts that I think this committee has heard before. Equifax had this information. In March, it learned that it had a vulnerable software in place in its public-facing website. There was a patch available. It was aware of it. It failed to implement it.

I think, importantly, it also failed in other respects. It failed to detect the presence of hackers in its network. I have seen reports that the hackers got in, in March. They didn't notice it until the end of July. So over 4 months, somehow they didn't know that there were thieves in their network. And another point is, they didn't realize that this data, 145 million person's information, was compromised.

I think that calls into question, and we have raised it in our complaints, serious questions of who was minding the store, putting the patch issue aside.

As I mentioned, we sued under our State data security regulations. And I will just highlight some of the regulations that are at issue in this case, to give you a sense of what our law provides. We allege Equifax failed to identify and assess reasonably foreseeable risks to the security of its information. It failed to evaluate and improve its existing safeguards.

Mr. ROTHFUS. The gentleman's time has expired.

Mr. KIHUEN. Thank you, Mr. Chairman.

Mr. ROTHFUS. The Chair recognizes the gentleman from Texas, Mr. Gonzalez, for 5 minutes.

Mr. GONZALEZ. Thank you, Mr. Chairman, and thank you, Ranking Member Waters.

Well, as a trial lawyer who represented consumers for 20 years, I certainly believe Equifax should be held liable and punished for their negligence. But knowing what we know now, with the multiple breaches from the credit reporting agency—and I guess this

question would go to Ms. McGee and Ms. Cable—would you support a direct cause of action against Equifax by consumers?

Ms. MCGEE. I will answer by saying, first of all, New York State law does not have under our data protection law an independent cause of action for consumers. It is not our intent to open that up, but that does then directly turn me to the arbitration issue, which is—for New York, when we saw that arbitration was going to be a barrier to justice for consumers who are trying to seek redress from the very entity that they had placed their sort of last hope when they traditionally had a data breach and now were victimized by that actual entity and then forced into an arbitration clause, if they wanted to avail themselves of any relief, we acted quickly to seek redress and the arbitration clause was removed.

It poses a real problem when consumers are hobbled in seeking rights in consumer protection because of these arbitration clauses. Our offices come out very strongly in statements condemning yesterday's decision and in other forced arbitration clauses, and that is a real problem.

Mr. GONZALEZ. But do you believe that they should have the capacity to bring their own claims?

Ms. MCGEE. At this point, under New York law, we don't. We don't provide that redress under New York law—

Mr. GONZALEZ. Do you think it is a good idea?

Ms. MCGEE. I think that, under certain circumstances, class actions can provide a way for a sea of change under law and can provide another way for companies to change the way that they do business. So as a generic matter, I personally don't think that it is a bad idea. But right now, I don't see any way in New York for there to be a change in that.

Mr. GONZALEZ. Fair enough. I guess the next question is to anyone on the panel is, how are we quantifying the damages? It seems like we can't get to that number anytime soon. How do we get there? At some point, how do we protect folks who had their information stolen from them? And it seems like it is just—we are looking into a crystal ball and we don't know where the end is.

How would you address that, Ms. Cable?

Ms. CABLE. I certainly, as a fellow litigator, appreciate that question. And speaking in generalities, in Massachusetts, one measure of damages—and certainly not the only—is the cost of placing, temporary lifting, and permanently lifting a security freeze. To do all three of those actions in Massachusetts would cost a consumer \$15 at one of the three bureaus, so \$45 at all three. Three million consumers in Massachusetts, presumably, had to pay that cost, and so I think that comes out to \$135 million in Massachusetts alone.

That is just one small measure that doesn't count identity theft or other forms of financial fraud that, as my co-panelists have highlighted, is very likely to occur here. I think establishing damages that may not have happened yet is either impossible or impracticable as a matter of law and it is what it is.

I think one solution would be establishing minimum statutory damages and allowing the consumer to seek either the higher of the actual or the minimum. I think the law can advance this issue forward by establishing some kind of measure for damages here.

Mr. GONZALEZ. Very well. And the reason I say that is because \$5,000 just seems nothing compared to some people can be damaged at such a high value. I guess my next question, and I hate to pick on all the lawyers, but I will address Ms. Moy. Which State has the most stringent protection for data breaches in the country?

Ms. MOY. So, again, with breaches, I think that when it comes to notification, many consumers feel that it is too late. So that the laws to look at for really strong protection for consumers are going to be the data security laws.

And some at this table have good ones. Massachusetts has a very strong one. New York has new cybersecurity regulations. Connecticut also recently has a good law, and Illinois. California, of course, is a good one to look at. Texas, actually, is an interesting State because it covers a broad set of information.

Mr. GONZALEZ. Which is changing, by the way. I don't know if you followed this last legislative session.

Ms. MCGEE. I am not aware of the changes. I will have to look into that.

Mr. GONZALEZ. Under DTPA—and consumer laws have been watered down recently. But I am curious—and you just told us—you just mentioned a few States that do have good laws. What States would you say do not? And I guess my time is up. Thank you very much.

Mr. ROTHFUS. The gentleman's time is expired.

The Chair recognizes the gentlewoman from Ohio, Mrs. Beatty, for 5 minutes.

Mrs. BEATTY. Thank you, Mr. Chairman. And thank you to our Ranking Member, Congresswoman Waters.

I really appreciate us having an opportunity to have this dialog and to have it with you as our eyewitnesses. And I don't want to take my time to repeat everything that has been said.

But let me certainly echo the displeasure that we have that Equifax could not be here, chose not to be here, chose not to sit and respond to something that has affected 143-plus-million individuals. I find that appalling that they are ignoring a request to come before this committee.

I am also saying, Mr. Chairman, I am disappointed that we don't have seats across the aisle filled. This is not a partisan issue. This is not about Democrats. This is about 143 million people having their entire life disrupted because of a company that had had some 57,000 complaints about misinformation, about inaccuracies on their credit reports.

And I am as upset as anyone else, because I tried to work with them. I actually offered a bill in the last session, and in this session, and if they would have spent more time working with me than against the bill that would allow consumers to get a free credit report, it would have been helpful.

But they didn't want to get a free credit score, because it is one thing to say, OK, once a year, we have a law now that you can get your annual report. But what happens when you go in to buy a home? What happens when they ask you what is your credit score?

And they did not want to even do it once a year to give them a free credit score. And so, I hope someone plays this tape back to them so they can understand that we represent hard-working

Americans. We represent people who want to have a better future. And when you have the breaches that they have had and you don't come to the table to respond to it, that is simply unacceptable.

I guess, as I am sitting here today, I believe one of the ways we can really get companies to focus on cybersecurity is to put in place a system where there is a monetary penalty for each person's data that is breached. You know, let them feel some of the consequences that 143 million people are experiencing.

When you think about—we have the data up here—one out of five consumers has had an error on their report. So there were already issues with them. There were already things that they knew that this could be a possibility, and what did they do? They ignored it. That is unacceptable.

So, let me ask you, what do you think about putting a penalty in where the Equifaxes or future Equifaxes would have to pay that? And what should that number be? Should it be \$1,000, should it be \$5,000, should it be a greater number?

Ms. Wu?

Ms. WU. Well, thank you, Congresswoman Beatty, and thank you for the question. And I completely agree there should be some sort of penalty when companies lose our data. You know, it is unacceptable. And in addition to the types of damages that Ms. Cable talked about, in terms of freezes and lifting, there is time spent, there is aggravation, there is being upset that your information is out there with thieves and you are potentially a victim next.

And that should all be compensated. You know, the maximum statutory damages under the Fair Credit Reporting Act is \$1,000. That was 40 years ago. It probably should be a lot greater than that.

Mrs. BEATTY. So should we be looking at legislation to make that number more in line with today's cost of living?

Ms. WU. Well, certainly increasing the statutory damages is something we would be in favor of. And as you know, there was the bill just the same day that Equifax announced its breach, there was a hearing on a bill to reduce those damages under the Fair Credit Reporting Act.

Mrs. BEATTY. Well, I think my time is up. So, Mr. Chairman, I yield back.

Mr. ROTHFUS. The gentlewoman yields back. The Chair recognizes the Ranking Member for unanimous consent requests.

Ms. WATERS. Thank you very much. I have a number of them, Mr. Chairman. I have 31 communications in support of 3755, the Comprehensive Consumer Credit Reporting Reform Act. We have—

Mr. ROTHFUS. Without objection.

Ms. WATERS —thank you—testimony that was written and sent to us today from Consumers Union.

Mr. ROTHFUS. Without objection.

Ms. WATERS. Two such documents.

Mr. ROTHFUS. Without objection.

Ms. WATERS. I have "Equifax Grip on Mortgage Data Squeezes Smaller Rivals" from the New York Times.

Mr. ROTHFUS. Without objection.

Ms. WATERS. From Salon, I have a communication.

Mr. ROTHFUS. Without objection.

Ms. WATERS. "Equifax Grip on Mortgage Data Squeezes Smaller Rivals," another one from the New York Times.

Mr. ROTHFUS. Without objection.

Ms. WATERS. Written questions for the record submitted by Democratic members for October 5th, Equifax hearing.

Mr. ROTHFUS. Without objection.

Ms. WATERS. Written statement asked to be submitted by FICO to this hearing.

Mr. ROTHFUS. Without objection.

Ms. WATERS. Press statement was released from CFPB, "Supervisory Highlights Focused on Problems Discovered with Credit Bureaus."

Mr. ROTHFUS. Without objection.

Ms. WATERS. Written statements for the record from the first Equifax hearing on October 5th.

Mr. ROTHFUS. Without objection.

Ms. WATERS. And information on CFPB's website about ID theft tools available to consumers.

Mr. ROTHFUS. Without objection.

Ms. WATERS. Thank you very much. I yield back.

Mr. ROTHFUS. There being no members remaining to question the panel, this concluded today's hearing. Without objection, all members will have 5 legislative days within which to submit additional written questions for the witnesses to the Chair, which will be forwarded to the witnesses for their response. I ask our witnesses to please respond as promptly as you are able.

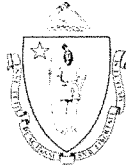
This hearing is adjourned. Thank you.

[Whereupon, at 3:42 p.m., the committee was adjourned.]



# **A P P E N D I X**

October 25, 2017



THE COMMONWEALTH OF MASSACHUSETTS  
OFFICE OF THE ATTORNEY GENERAL  
ONE ASHBURTON PLACE  
BOSTON, MASSACHUSETTS 02108

MAURA HEALEY  
ATTORNEY GENERAL

(617) 727-2200  
(617) 727-4765 TTY  
www.mass.gov/ago

**Prepared Statement of Sara Cable  
Assistant Attorney General and Director of Data Privacy & Security  
Consumer Protection Division  
Office of the Massachusetts Attorney General**

**Before the House of Representatives Financial Services Committee**

**Continuation of Hearing Entitled "Examining the Equifax Data Breach"**

**October 25, 2017**

**I. Introduction**

Chairman Hensarling, Ranking Member Waters, and members of the Committee, thank you for inviting me to testify today regarding the recent Equifax breach. I am an Assistant Attorney General for the Massachusetts Attorney General's Office, and the Director of Data Privacy and Security for its Consumer Protection Division. On September 19, our Office filed the first state enforcement suit against Equifax. Our goal is to hold the company accountable for the harms the breach has caused nearly 3 million Massachusetts consumers – half of our adult population.<sup>1</sup>

We sued Equifax because, in our view, the company left hundreds of millions of records consisting of consumers' most sensitive personal information vulnerable to hackers, despite knowing for months that its website was insecure. Among other things, we allege that Equifax violated the Massachusetts Consumer Protection Act and Data Security regulations, which require Equifax to develop, implement, and maintain reasonable administrative, technological, and physical safeguards to protect consumers' data from foreseeable harm. We also allege that Equifax failed to promptly notify consumers that their information was compromised, in violation of the Massachusetts Data Breach Law, and that it compounded consumers' harm by charging consumers to implement security freezes necessitated by its own mistakes. Our view is that Equifax could have and should have prevented this breach.

The implications of the Equifax breach go far beyond the failure of one company to secure consumer data. While the Equifax breach may be unique in its scope, the failure to reasonably secure consumers' data from foreseeable threats is an ongoing challenge for organizations in every sector. The Equifax breach also raises broader questions about the collection, sale, and use of consumer data in the consumer reporting industry. I want to highlight three key points.

---

<sup>1</sup> A copy of our Complaint is attached as **Exhibit 1**.



First, it appears to us that organizations that profit off consumers' data are not taking reasonable steps to secure it from foreseeable threats of compromise. Over the last ten years, our Office has received notice of over 19,000 data breaches impacting millions of Massachusetts residents. The failure by a business to take seriously the security of the consumer data while profiting off that data it is unfair and undermines the consumer trust necessary for a thriving information-based economy. Stronger laws coupled with more aggressive enforcement are needed to ensure that organizations are incentivized to protect consumers' data from unauthorized use or access.

Second, consumers lack adequate protections and recourse when their data is compromised – an increasing probability for nearly every US consumer. Consumers currently have to jump through too many hoops and pay too much money to freeze their credit files – one of the best ways to protect themselves after a data breach. Consumers likewise face too many challenges in obtaining compensation for losses caused by an entity's failure to protect their data. Consumers must be able to easily and quickly freeze their credit files for free, without giving up any legal rights or having to further share personal information. Consumers also should be able to seek legal redress and compensation – in addition to any other monetary losses they may suffer – for the time and money spent responding to a breach. Because ascertaining actual damages may be difficult, consumers should be entitled to seek (the higher of) actual damages, or meaningful statutory damages when their information is compromised by a business's failure to reasonably secure it.

Third, consumers lack meaningful control over who gets their data, the circumstances under which their data is taken, and what is being done with their data. According to Equifax, the breached data did not come from its core consumer or commercial credit reporting databases, but was a separate cache stored elsewhere. It is not yet clear how Equifax obtained this data or what it was used for. Many consumers did not knowingly choose to give this data to Equifax and did not knowingly choose to do business with them, yet now have to suffer the consequences of Equifax's mistakes. Consumers must have more control over who is collecting their personal data and how it is being used so that they can assess the risks of sharing it.

## **II. Companies Continue to Struggle to Safeguard Consumer Data from Foreseeable and Preventable Risks.**

### ***A. The Massachusetts Data Breach Law and Data Security Regulations Protect Consumers from Data Breaches.***

Massachusetts has among the strongest data protection laws nationally. Together, its laws and regulations require entities that own or license "personal information"<sup>2</sup> of Massachusetts residents to develop, implement, and maintain minimum security safeguards to protect such

---

<sup>2</sup> In Massachusetts, "personal information" is defined by statute to mean a resident's first name and last name, or first initial and last name, in combination with any one or more of the following data elements: (a) social security number; or (b) driver's license number or state-issued identification card number; or (c) financial account number or credit or debit card number, with or without any required security code. See M.G.L. c. 93H, §1 (attached as **Exhibit 2**).

information from foreseeable threats or hazards and from unauthorized access or use.<sup>3</sup> If such information is breached, Massachusetts law obligates entities to provide prompt notice to affected residents and state agencies, including the Attorney General.<sup>4</sup>

My Office has ten years of experience enforcing these laws to protect consumers from data breaches and violations of their privacy. Over this time, we have received notice of over 19,000 data breaches, affecting nearly every sector of the economy. We have investigated countless of these incidents, and enforced the laws against multiple entities that fail to employ reasonable safeguards in the face of foreseeable threats to consumer's personal information. Because of this work, Massachusetts is regarded as a leader in protecting the security and privacy of consumer data.

***B. The Massachusetts Attorney General Seeks to Hold Equifax Accountable.***

Measured against this enforcement experience, the Equifax breach is one of the worst we have seen. That is why our Office has filed the nation's first enforcement suit against Equifax. We seek to hold Equifax accountable and seek redress for consumers.

As this Committee has previously learned, from March 7, 2017 through July 29, 2017, Equifax left sensitive and private consumer information exposed to intruders by relying on outdated versions of computer code ("Apache Struts") that it knew or should have known was vulnerable to exploitation. Still unknown third parties infiltrated Equifax's computer system through the company's public, online "Dispute Portal." The hackers were present in Equifax's system from at least May 13, 2017 through the end of July 2017.

This computer code vulnerability was publicly known and fixes were posted on at least two U.S. Government websites, among other industry sources. Nonetheless, we allege that Equifax failed to implement the recommended fixes or other steps to prevent the hackers from gaining access.

As a result, we allege that hackers were able to get into Equifax's internal network. But this is not the only thing that we allege Equifax did wrong. Once inside, the hackers were able to roam freely in Equifax's network for months, without Equifax noticing their presence or kicking them out. Over this time, the hackers gained access to hundreds of millions of data records consisting of the most sensitive personal data of 145 million American – all without Equifax noticing.

In our Complaint, we claim that Equifax did not develop, implement, or maintain safeguards required by Massachusetts law to protect consumer data. Such minimum safeguards relate to, among other things, the installation of software security patches, the regular monitoring of computer systems, and the detection and prevention of security systems failures. We also allege that Equifax violated Massachusetts law by keeping hundreds of millions of records containing

---

<sup>3</sup> See M.G.L. c. 93I and Title 201 of the Code of Massachusetts Regulations, section 17.00 *et seq.* (201 C.M.R. 17.00 *et seq.*) (attached as **Exhibit 3** and **Exhibit 4**).

<sup>4</sup> See M.G.L. c. 93H (**Exhibit 2**).

consumers' sensitive personal information in unencrypted form and not protected through other methods.

The Equifax breach is notable because of its scope, but it is not unique. Data breaches remain a threat to consumers and businesses alike. All too often, we see data breaches that result when a company fails to develop a security program, fails to comply with its security policies, ignores security warnings, neglects to apply critical software patches, or fails to take other reasonable measures to safeguard consumers' information. These all-too-common security lapses are inevitably exploited by cybercriminals hunting for personal information. In brief, our experience shows that there is much room for improvement.

***C. To the Extent Any Federal Data Security Standard is Considered, It Should Not Preempt or Undercut State Law.***

The Equifax breach may bring into consideration whether a national data breach notice and data security standard is warranted. As noted, Massachusetts has among the strongest data security and breach laws in the country. My Office has serious concerns to the extent any federal standard seeks to set weaker standards than those that currently exist for Massachusetts consumers and that would preempt existing or future state law in this field. States are active, agile, and experienced enforcers of their consumers' data security and privacy, and need to continue to innovate as new risks emerge.

To the extent any such national standard is considered, it must contain strong, minimum data security standards that do not erode existing state protections. As described in more detail in prior comments to the U.S. House Subcommittee on Commerce, Manufacturing, and Trade in March 2015 (attached as **Exhibit 5**), any national standard should, at a minimum:

- Serve as a floor of protections that a state may exceed;
- Contain strong, defined, but flexible data security standards;
- Ensure sufficient enforcement mechanisms, including by State Attorneys General;
- Contain meaningful penalty provisions to deter future violations and ensure violations of the law are not treated simply as the cost of doing business;
- Impose clear requirements for timely and effective consumer notice procedures; and
- Preserve the ability of consumers to seek legal redress for damages for losses resulting or caused by a breach, including minimum statutory damages, as ascertaining individual losses may not be possible or practical.

Given the near-constant threat of data breaches to every American consumer and the risks consumers now face due to the Equifax breach, any national standard must preserve the current level of protections enjoyed by consumers and the enforcement powers of the State Attorneys General to avoid lowering the bar of security and breach standards, and an associated drop in consumer confidence in the marketplace. I respectfully refer the Committee to the standards

outlined in the Massachusetts Data Breach Notice Law (M.G.L. c. 93H) and the Massachusetts Data Security Standards (201 C.M.R. 17.00 *et seq.*), as a model for any national standard.

### III. Consumers Need More Meaningful and Accessible Protections When Their Data is Breached.

We allege in our complaint that not only did Equifax fail to prevent a foreseeable breach, it also failed to notify consumers promptly and erected unnecessary hurdles in offering the assistance necessary for consumers to protect themselves from Equifax's own mistakes.

As we allege, the company knew about the breach around July 29, 2017 and should have known then or soon after it had a notification obligation under Massachusetts law, yet it did not notify the Commonwealth or consumers until September 7, 2017. This nearly six-week delay gave the hackers plenty of time, even after they could no longer access Equifax's systems, to use the stolen data before consumers could take steps to protect themselves, such as by freezing their credit files.

We further allege that Equifax compounded this risk by failing to make readily available various protections it was uniquely positioned to offer consumers to mitigate the risk of harm caused by its own mistakes. It charged consumers to place security freezes,<sup>5</sup> refused to arrange for free security freezes at other national CRAs, failed to offer consumers free credit and fraud monitoring beyond one year, and failed to ensure adequate call center staffing and availability of online services in the days following the announcement of the breach.

We have also already begun to receive complaints of identity theft and fraud. Because identity theft can strike at any time, it is reasonable to assume that consumers will be subject to this risk for years.

The aftermath of the Equifax breach highlights numerous areas for policy development and reform to better protect consumers from the increasing risk of data breaches. Some basic reforms we have proposed on the state level include **free and fast security freezes**. Consumers must be able to easily and quickly freeze their credit files to prevent new accounts from being opened in their names, and they should not pay a penny for a company's data security mistakes.

Similarly, there should be a **"one-stop shop" for security freezes**. We have heard from numerous consumers of the frustrating difficulties they faced in navigating the security freeze processes at the three separate CRAs after the Equifax breach. Section 605A of the Federal Fair Credit Report Act obligates a CRA that receives a request for a fraud alert to notify all other CRAs of that alert. A similar mechanism for a "one-stop shop" should be mandated for security freezes.

---

<sup>5</sup> A security freeze is a mechanism by which a CRA prevents a party from accessing a consumer's credit file without the consumer's consent. It is an important protection to consumers whose personal information is compromised in a data breach because it makes it more difficult for an identity thief to open new accounts in a consumer's name. Massachusetts law permits, but does not require, a consumer reporting agency to charge the consumer a "reasonable fee, not to exceed \$5," to place, lift, or remove a freeze on the consumer's credit report. See M.G.L. c. 93, § 62A.

Consumers should also get access to more **free copies of credit reports after a data breach**. Despite the increasing prevalence of data breaches, consumers are unable to monitor their credit reports for free when their information is compromised by a breach. Instead, consumers must use up their one free annual report to check for fraud after being notified of a breach, or pay the CRA for additional reports. This should be changed. Consumers should have free access to their credit reports after a breach to monitor and respond to evidence of unauthorized activity.

If a CRA is breached, it should provide consumers with **free, “no strings attached” credit monitoring for at least five years**. CRAs maintain vast volumes of the very consumer data sought by criminals to commit identity theft and financial fraud. They are also uniquely positioned to monitor consumers’ credit files for such unlawful activities. Given this, they should be required to provide free credit monitoring for consumers affected by a breach at their organization for at least five years. Further, a CRA should not profit from such credit monitoring and consumers should not be required to waive any legal rights – including the right to bring a private action – for availing themselves of the service.

Finally, consumers must be able to **seek full legal redress for any damages** resulting from the data breach, including but not limited to financial losses from identity theft. Entities that allow consumers’ information to be compromised should not be allowed to compel consumers to arbitrate their claims. Consumers must also be able to seek legal redress for losses resulting or caused by a breach, including minimum statutory damages, as ascertaining individual losses may not be possible or practical.

#### **IV. Consumers Need More Control Over How Their Data is Used by the Consumer Reporting Industry.**

The Equifax breach raises the larger problem that consumers lack control and knowledge over how the consumer reporting industry is collecting and using their personal data. According to Equifax, the compromised data was not within Equifax’s core consumer or commercial credit reporting databases, but was a different cache of data, stored separately. It is not yet clear how Equifax obtained this consumer data, why they had it, what it was used for, and with whom it was shared. A theme of the anger and confusion consumers have expressed to our Office relates to how Equifax could have had their personal data in the first place, where the consumer had no knowing relationship with Equifax, and made no knowing decision to give it their data.

Consumers’ personal data is their own. Consumers need and deserve control and choice over who has their data. Where decisions of socio-economic consequence are made based on that data, consumers should be aware of what data is disclosed, to whom, and for what purposes. States are on the front lines of consumers’ privacy protection, and are best positioned to innovate in this area. At the state level, we are proposing legislation that would require companies to get a consumer’s prior written permission before accessing his or her credit report or credit score. In our view, this is a modest step to ensure consumers have more control over their information so that they can make smarter decisions about who has it and for what ends it is being used. To the extent federal policy along the above lines is not contemplated, then the Federal Fair Credit Reporting Act should be amended to give the States more freedom to enact stronger protections for its consumers.

**V. Conclusion**

I appreciate this opportunity to share these views with the Committee, and thank the Committee for its careful examination of these important issues. Please do not hesitate to contact me for any additional detail, clarity or with any questions you may have.

## **Exhibit 1**

COMMONWEALTH OF MASSACHUSETTS

SUFFOLK, ss.

SUPERIOR COURT  
CIVIL ACTION NO.

COMMONWEALTH OF MASSACHUSETTS,

Plaintiff,

v.

EQUIFAX, INC.

Defendant.

COMPLAINT

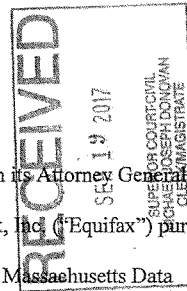
JURY TRIAL REQUESTED

INTRODUCTION

1. The Commonwealth of Massachusetts, by and through its Attorney General Maura Healey ("Commonwealth"), brings this action against Equifax, Inc. ("Equifax") pursuant to the Massachusetts Consumer Protection Act (G.L. c. 93A) and the Massachusetts Data Security Law (G.L. c. 93H).

2. Equifax is one of three primary national credit-reporting bureaus in the United States. Equifax collects and maintains data regarding more than 820 million consumers worldwide, including at least 3,000,000 in Massachusetts. The personal data that Equifax holds touches upon virtually every aspect of a consumer's profile in the marketplace.

3. Equifax is a gatekeeper for consumers' access to socioeconomic opportunity and advancement. Every day, businesses across the country rely on Equifax's credit profiles to make decisions as to the credit worthiness of consumers. This information impacts many of the most important decisions in the lives of consumers—for instance, whether consumers can buy a house, obtain a loan, lease a vehicle, or even get a job.





4. Consumers do not choose to give their private information to Equifax, and they do not have any reasonable manner of preventing Equifax from collecting, processing, using, or disclosing it. Equifax largely controls how, when, and to whom the consumer data it stockpiles is disclosed. Likewise, consumers have no choice but to rely on Equifax to protect their most sensitive and personal data. Accordingly, it was and is incumbent on Equifax to implement and maintain the strongest safeguards to protect this data. Equifax has failed to do so.

5. From at least March 7, 2017 through July 30, 2017, a period of almost five months, Equifax left at least 143 million consumers' sensitive and private information exposed and vulnerable to intruders by relying on certain open-source code (called "Apache Struts") that it knew or should have known was insecure and subject to exploitation. Although patches, workarounds, and other fixes for the vulnerability were available and known to Equifax as of March 7, 2017, Equifax failed to avail itself of these remedies or employ other compensating security controls, such as encryption or multiple layers of security, that were sufficient to protect consumers' personal data.

6. As a result, intruders were able to access Equifax's computer system from at least May 13, 2017 through July 30, 2017, and potentially stole the sensitive and personal information of 143 million consumers (the "Data Breach"). The Data Breach, which Equifax first disclosed to the public on September 7, 2017, exposed to still-unknown persons some of the most sensitive and personal data of Massachusetts residents, including full names, social security numbers, dates of birth, addresses, and for some consumers, credit card numbers, driver's license numbers, and/or other unknown, personally-identifiable information.

7. Equifax could have—and should have—prevented the Data Breach had it implemented and maintained reasonable safeguards, consistent with representations made to the

public in its privacy policies, industry standards, and the requirements of Massachusetts law. Equifax did not do so.

8. By failing to secure consumer information, Equifax exposed over half of the adult population of Massachusetts to the risks of identity theft, tax return scams, financial fraud, health identity fraud, and other harm. Affected consumers have spent, and will continue to spend, money, time, and other resources attempting to protect against an increased risk of identity theft or fraud, including by placing security freezes over their credit files and monitoring their credit reports, financial accounts, health records, government benefit accounts, and any other account tied to or accessible with a social security number. The increased risk of identity theft and fraud as a result of the Data Breach also has caused Massachusetts consumers substantial fear and anxiety and likely will do so for many years to come.

9. Given the nature of Equifax's business, the sensitivity and volume of the data in which it traffics, and the serious consequences to consumers when that data is exposed, its failure to secure this information constitutes a shocking betrayal of public trust and an egregious violation of Massachusetts consumer protection and data privacy laws. As Equifax's own Chairman and Chief Executive Officer admitted, the Data Breach "strikes at the heart of who we are and what we do."

10. By this action the Commonwealth seeks to ensure that Equifax is held accountable, and not allowed to prioritize profits over the safety and privacy of consumers' sensitive and personal data. The Commonwealth seeks civil penalties, disgorgement of profits, restitution, costs, and attorney's fees, as available under G.L. c. 93A and G.L. c. 93H. The Commonwealth also seeks all necessary, appropriate, and available equitable and injunctive

relief to address, remedy, and prevent harm to Massachusetts residents resulting from Equifax's actions and inactions.

**THE PARTIES**

11. The Plaintiff is the Commonwealth of Massachusetts, represented by its Attorney General, who brings this action in the public interest pursuant to G.L. c. 93A, § 4, and G.L. c. 93H, § 6.

12. Defendant Equifax, Inc. is a publicly-traded Georgia corporation with its principal place of business at 1550 Peachtree Street N.E., Atlanta, Georgia.

**JURISDICTION, AUTHORITY, AND VENUE**

13. The Attorney General is authorized to bring this action, in this Court, under G.L. c. 93A, § 4, and G.L. c. 93H, § 6.

14. This Court has jurisdiction over the subject matter of this action by virtue of G.L. c. 93A, § 4, and G.L. c. 212, § 4.

15. This Court has personal jurisdiction over Equifax under G.L. c. 223A, § 3, including because Equifax has engaged in business with Massachusetts entities, and because Equifax's actions and inactions have affected Massachusetts residents.

16. Venue is proper in Suffolk County under G.L. c. 93A, § 4, as Equifax "has no place of business within the commonwealth," and under G.L. c. 223, § 5, as the Commonwealth is the plaintiff.

17. The Commonwealth notified Equifax of its intent to bring this action at least five days prior to the commencement of this action, as required by G.L. c. 93A, § 4.

**FACTS*****Equifax's Business***

18. Equifax's business centers on the collection, processing, and sale of information about people and businesses. According to its website, Equifax is a "global information solutions company" that "organizes, assimilates, and analyzes data on more than 820 million consumers and more than 91 million businesses worldwide, and its database includes employee data contributed from more than 7,100 employers." Equifax employs approximately 9,900 people worldwide.

19. As part of its business, Equifax creates, maintains, and sells "credit reports" and "credit scores" regarding individual consumers, including Massachusetts residents. Credit reports can contain, among other things, an individual's full social security number, current and prior addresses, age, employment history, detailed balance and repayment information for financial accounts, bankruptcies, judgments, liens, and other sensitive information. The credit score is a proprietary number, derived from a credit report and other information, that is intended to indicate relative to other persons whether a person would be likely to repay debts.

20. Third parties use credit reports and credit scores to make highly consequential decisions affecting Massachusetts consumers. For instance, credit scores and/or credit reports are used to determine whether an individual qualifies for a mortgage, car loan, student loan, credit card, or other form of consumer credit; whether a consumer qualifies for a certain bank account, insurance, cellular phone service, or cable or internet service; the individual's interest rate for the credit they are offered; the amount of insurance premiums; whether an individual can rent an apartment; and even whether an individual is offered a job.

*The Data Breach*

21. At all relevant times, Equifax maintained a publicly available website at [www.equifax.com](http://www.equifax.com).

22. Within that website are various publicly available web pages directed to consumers, including Massachusetts residents. Among those web pages is one through which Equifax invites consumers to submit information to initiate and support a formal dispute of information in their credit reports (the “Dispute Portal”).

23. Equifax maintained consumer names, addresses, full social security numbers, dates of birth, and for some consumers, driver’s license numbers and/or credit card numbers of at least 143 million consumers, including nearly 3 million Massachusetts residents, in computer tables, databases, or files that were accessible (directly or indirectly) through the Dispute Portal (the “Exposed Information”). The Exposed Information, which included “Personal Information” as defined in G.L. c. 93H, § 1, and 201 CMR. 17.02, was not limited to the sensitive and personal information of those consumers who had used the Dispute Portal, but encompassed a larger group of consumers on whom Equifax held information.

24. Despite being accessible through a publicly available website, the Exposed Information was not “encrypted” on Equifax’s systems as defined in 201 CMR 17.02.

25. Starting on or about May 13, 2017 through July 30, 2017, unauthorized third parties infiltrated Equifax’s computer system via the Dispute Portal. Once in, the parties accessed and likely stole (i.e. “exfiltrated”) the Exposed Information from Equifax’s network.

*Equifax Ignored Numerous Signs that Its System  
—and the Consumers’ Data Stored Therein—Was Vulnerable to Hackers*

26. According to a statement Equifax published online at <https://www.equifaxsecurity2017.com> on or about September 13, 2017, the Data Breach resulted when “criminals exploited a U.S. website application vulnerability. The vulnerability was Apache Struts CVE-2017-5638.”

27. Apache Struts is a piece of computer code used for creating web applications; i.e. a computer program that runs in a web browser.

28. At all relevant times, Equifax used Apache Struts, in whole or in part, to create, support, and/or operate its Dispute Portal.

29. As “open-source code,” Apache Struts is free and available for anyone to download, install, or integrate into their computer system. Apache Struts, like many other pieces of open-source code, comes with no warranties of any kind, including warranties about its security. Accordingly, it is incumbent on companies that use Apache Struts—like Equifax—to assess whether the open-source code is appropriate and sufficiently secure for the company’s purposes and that it is kept up-to-date and secure against known vulnerabilities.

30. There are, and at all relevant times have been, multiple well-known resources available to support companies relying on open-source code, including Apache Struts. These resources publicly announce to users when security vulnerabilities in the open-source code are discovered and verified, including in Apache Struts, compare the associated risks of such vulnerabilities, and propose fixes.

31. For example, the Apache Software Foundation (“Apache”), a non-profit corporation, releases updated versions of Apache Struts to “patch” it against verified security vulnerabilities. Apache also releases Security Bulletins on its website regarding security flaws in

Apache Struts, noting the nature of the vulnerability and ways to resolve it. Since 2007, Apache has posted at least 53 such security bulletins for Apache Struts.

32. Similarly, the U.S. Department of Commerce’s National Institute of Standards and Technology (“NIST”) maintains a free and publicly available National Vulnerability Database (“NVD”) at <http://nvd.nist.gov>. Using the NVD, NIST identifies security vulnerabilities, including in open-source code, the risks they pose, and ways to fix them, including as to security vulnerabilities in Apache Struts.

33. Likewise, the MITRE Corporation, a “not-for-profit organization that operates research and development centers sponsored by the [United States] federal government,”<sup>1</sup> also identifies code security vulnerabilities, including vulnerabilities in Apache Struts, using a Common Vulnerabilities and Exposures (“CVE”) Identifier. According to MITRE, the CVE Identifier is the industry standard for identifying publicly known cyber security vulnerabilities. MITRE maintains a database of CVE identifiers and the vulnerabilities to which they correspond, which is publicly accessible without cost online at <https://cve.mitre.org> (the “Vulnerability Database”).

34. On March 7, 2017, Apache published notice of a security vulnerability in certain versions of Apache Struts in its online security bulletins S2-045 and S2-046 (the “Apache Security Bulletins”). **Exhibit 1** (<https://cwiki.apache.org/confluence/display/WW/S2-045> last visited September 19, 2017) and **Exhibit 2** (<https://cwiki.apache.org/confluence/display/WW/S2-046> last visited September 19, 2017). The vulnerability was assigned the CVE identifier CVE-2017-5638 (the “March Security Vulnerability”).

---

<sup>1</sup> <https://www.mitre.org/>.

35. Directed to “All Struts2 developers and users,” the Apache Security Bulletins warned that the software was vulnerable to “Remote Code Execution,” or “RCE.” RCE refers to a method of hacking a public website whereby an online attacker can send computer code to the website that allows the attacker to infiltrate (that is, gain access to), and run commands on the website’s server (the computer that stores the information that supports the website).

36. The Apache Security Bulletins assigned the March Security Vulnerability a “maximum security rating” of “critical.” Apache recommended that users update the affected versions of Apache Struts to fix the vulnerability, or to implement other specific workarounds to avoid the vulnerability. **Exhibits 1 and 2.**

37. NIST also publicized the March Security Vulnerability in its NVD on or about March 10, 2017. **Exhibit 3** (<https://nvd.nist.gov/vuln/detail/CVE-2017-5638>, last visited September 19, 2017) (the “NIST Notice”). NIST noted that the severity of the vulnerability was an overall score of 10.0 on two different versions of a scale called the Common Vulnerability Scoring System (“CVSS”). A score of 10.0 is the highest possible severity score on either scale. The NIST Notice also stated that an attack based on the vulnerability “[a]llows unauthorized disclosure of information,” would be low in complexity to accomplish, and would not require the attacker to provide authentication (for example, a user name and password) to exploit the vulnerability. The NIST Notice also documented over twenty other website resources for advisories, solutions, and tools related to the March Security Vulnerability and how to patch or fix it.

38. Following the NIST Notice, the United States Computer Emergency Readiness Team (“US CERT”) issued a security Bulletin (Bulletin (SB17-079)) on March 20, 2017, calling out the March Security Vulnerability as a “High” severity vulnerability (“US CERT Alert”).



**Exhibit 4** (excerpts from <https://www.us-cert.gov/ncas/bulletins/SB17-079>, last visited September 19, 2017) (relevant entry highlighted).

39. Likewise, MITRE included the March Security Vulnerability in the Vulnerability Database and documented various external website references to the March Security Vulnerability. **Exhibit 5** (<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5638>, last visited September 19, 2017).

40. In the days following the public disclosure of the March Security Vulnerability by Apache, media reports claimed that hackers were exploiting the March Security Vulnerability against numerous companies, including banks, government agencies, internet companies, and other websites.

41. As Equifax disclosed on its website on or about September 13, 2017, the Data Breach occurred as a result of the exploitation of the March Security Vulnerability by hackers.

42. As of or soon after March 7, 2017, Equifax knew or should have known, by virtue of multiple public sources but at least one or all of the Apache Security Bulletins, the NIST Notice, the US CERT Alert, and the Vulnerability Database (as well as one or all of the various collateral sources referenced in the foregoing), that the March Security Vulnerability existed in Apache Struts.

43. Indeed, in a notice on the website <https://www.equifaxsecurity2017.com/>, Equifax stated that “Equifax’s Security organization was aware of this vulnerability” in Apache Struts in early March 2017.

44. As of or soon after March 7, 2017, Equifax knew or should have known, by virtue of multiple public sources but at least one or all of the Apache Security Bulletins, the NIST Notice, the US CERT Alert, and the Vulnerability Database (as well as one or all of the various

collateral sources referenced in the foregoing), that the implementation of Apache Struts it employed on its websites, including without limitation, the Dispute Portal was susceptible to the March Security Vulnerability.

45. As of or soon after March 7, 2017, Equifax knew or should have known, by virtue of multiple public sources but at least one or all of the Apache Security Bulletins, the NIST Notice, the US CERT Alert, and the Vulnerability Database (as well as one or all of the various collateral sources referenced in the foregoing), that it was vulnerable to unauthorized access to sensitive and personal consumer information by exploitation of the March Security Vulnerability by hackers.

46. Until at least July 30, 2017, and during the Data Breach, Equifax continued to use an Apache Struts-based web application that was susceptible to the March Security Vulnerability for its Dispute Portal.

47. Until at least July 30, 2017, and during the Data Breach, Equifax failed to employ successfully recommended fixes or workarounds, otherwise patch or harden its systems, or put in place any compensating controls sufficient to avoid the March Security Vulnerability, safeguard the Exposed Information, or prevent the Data Breach.

48. In addition, until at least July 29, 2017, and during the Data Breach, Equifax did not detect and/or appropriately respond to evidence that unauthorized parties were infiltrating its computer systems and had access to the Exposed Information; and/or did not detect or appropriately respond to evidence that those parties were exfiltrating the Exposed Information out of Equifax's computer system.

49. As a result of Equifax's actions and inactions, the Data Breach occurred, and hackers were able to access and likely stole the sensitive and personal data of 143 million consumers, including of Massachusetts consumers.

***Equifax's Security Program Fell Short of Its  
Promises to Consumers and Massachusetts Law***

50. At all relevant times, Equifax promised the public that safeguarding consumers' sensitive, personal information is "a top priority."

51. At all relevant times on its Privacy Policy, available through a hyperlink at the bottom of each page of its public website, Equifax represented to the public:

We have built our reputation on our commitment to deliver reliable information to our customers (both businesses and consumers) and to protect the privacy and confidentiality of personal information about consumers. We also protect the sensitive information we have about businesses. Safeguarding the privacy and security of information, both online and offline, is a top priority for Equifax.

52. Equifax likewise represented to consumers that it would keep all of their credit information, including that which consumers submitted through the Dispute Portal, secure. In its "Consumer Privacy Policy for Personal Credit Reports," accessible at <http://www.equifax.com/privacy/personal-credit-reports>, Equifax represented that it has "reasonable, physical, technical and procedural safeguards to help protect your [i.e. consumers'] personal information."

53. By failing to patch or otherwise address the March Security Vulnerability, detect the hackers in their network, prevent them from accessing and stealing the Exposed Information, and otherwise failing to safeguard the Exposed Information, as set forth in paragraphs 21 to 49 herein, Equifax failed to live up to its representations to the public.

54. Equifax also failed to comply with Massachusetts Law.

55. The Massachusetts Data Security Regulations, promulgated pursuant to G.L. c. 93H, § 2(a), went into effect on March 1, 2010. The objectives of the Data Security Regulations are to “insure the security and confidentiality of customer information in a manner fully consistent with industry standards; protect against anticipated threats or hazards to the security or integrity of such information; and protect against unauthorized access to or use of such information that may result in substantial harm or inconvenience to any consumer.” G.L. c. 93H, § 2(a).

56. The Data Security Regulations “establish minimum standards to be met in connection with the safeguarding of personal information contained in both paper and electronic records.” 201 CMR 17.01(1). These minimum standards include, among others, the development, implementation, and maintenance of a comprehensive written information security program (a “WISP”) that contains enumerated, minimum safeguards to secure personal information owned or licensed by the entity. See 201 CMR 17.03.

57. The Data Security Regulations also require that an entity “establish[] and maint[ain] . . . a security system covering its computers” that contains certain minimum enumerated safeguards to prevent security compromises. See 201 CMR 17.04.

58. By failing to patch or otherwise sufficiently address the March Security Vulnerability, detect and appropriately respond to the presence of unauthorized parties in its network, prevent those parties from accessing and/or stealing the Exposed Information, and/or safeguard the Exposed Information, as set forth in paragraphs 21 to 49 herein, Equifax failed to develop, implement, or maintain a WISP that met the minimum requirements of the Data Security Regulations, 201 CMR 17.03 and 17.04.

59. In addition, the Data Security Regulations required Equifax to go beyond these minimum requirements and develop, implement, or maintain in its WISP additional safeguards that were “appropriate to” the “size, scope and type of business” of Equifax, the “amount of resources available to [it],” the “amount of stored data,” and “the need for security and confidentiality of both consumer and employee information.” 201 CMR 17.03(1).

60. Equifax is a large, sophisticated, multinational company of nearly 10,000 employees and billions of dollars in annual revenue whose primary business consists of acquiring, compiling, analyzing, and selling sensitive and personal data. Equifax holds the personal information and other personal data of more than 820 million consumers internationally—more than twice the population of the United States. This includes information that is sought after by hackers because it can be used to commit identity theft and financial fraud. As such, the Data Security Regulations required Equifax to implement administrative, technical, and physical safeguards that substantially exceed the minimum standards set forth in the Data Security Regulations, and which are at least consistent with industry best practices.

61. For example, and without limitation, Equifax’s size, scope and type of business, the amount of resources available to it, the amount of stored data, and the need for security and confidentiality of both consumer and employee information made it “appropriate” and necessary under the Data Security Rules for Equifax to have encrypted any Personal Information that was accessible via the publicly accessible, and vulnerable, Dispute Portal. It was also “appropriate” and necessary for Equifax to have maintained multiple layers of security sufficient to protect personal information stored in its system should other safeguards fail. By failing to do so, Equifax failed to comply with 201 CMR 17.03(1).

*Equifax Delayed Notifying the Public of the Data Breach*

62. Chapter 93H requires covered entities to report data breaches to the Commonwealth, including the Attorney General's Office and the Office of Consumer Affairs and Business Regulation, "as soon as practicable and without unreasonable delay, when such person . . . (1) knows or has reason to know of a breach of security [as that term is defined in G.L. c. 93H, § 1(a)], or (2) when the person or agency knows or has reason to know that the personal information of such resident was acquired or used by an unauthorized person or used for an unauthorized purpose[.]" G.L. c. 93H, § 3(b).

63. As of or soon after July 29, 2017, Equifax knew or should have known that the "personal information" (as defined in G.L. c. 93H, § 1(a)) of at least one Massachusetts resident was acquired by an unauthorized person, and/or of a "breach of security," and that it thus had a duty to provide notice to the Attorney General's Office and the Office of Consumer Affairs and Business Regulation under chapter 93H, § 3(b) "as soon as reasonably practicable and without unreasonable delay."

64. Equifax delayed providing notice to the Attorney General or the Office of Consumer Affairs and Business Regulation until September 7, 2017. Equifax thus failed to provide timely notice under chapter 93H, § 3(b).

65. Chapter 93H, § 3(b) also requires an entity to provide timely written notice, with content specified by § 3(b), of a reportable data breach to each affected consumer. Such notice, when promptly given, allows the consumer to take steps to protect him or herself from identity theft, fraud, or other harm that may result from the breach.

66. Under chapter 93H, § 1, a breached entity may provide "substitute notice" to consumers "if the person . . . required to provide notice demonstrates that the cost of providing

written notice will exceed \$250,000, or that the affected class of Massachusetts residents to be notified exceeds 500,000 residents, or that the person . . . does not have sufficient contact information to provide notice.” Substitute notice consists of all three of the following: (1) email notice to the extent the entity has email addresses for the affected residents, (2) a “clear and conspicuous posting of the notice on the home page” of the notifying entity and (3) “publication in or broadcast through media or medium that provides notice throughout the commonwealth.” G.L. c. 93H, §1.

67. Equifax knew or should have known as of or soon after July 29, 2017, that it met the threshold for being able to provide “substitute notice” as defined in chapter 93H, § 1.

68. Despite this, Equifax did not then avail itself of any element of the substitute notice process but instead delayed notifying the public of the Data Breach for nearly six weeks, until September 7, 2017, through a website posting. Equifax thus failed to provide timely notice to affected consumers as required by chapter 93H, § 3(b).

***Equifax’s Actions and Inactions in Connection with the Data Breach Have Created, Compounded, and Exacerbated the Harms Suffered by the Public***

69. The Attorney General is not required to demonstrate harm to consumers in order to enforce the Data Breach Notice Law (G.L. c. 93H), the Data Security Regulations (201 CMR 17.00–17.05), or the Consumer Protection Act (G.L. c. 93A).

70. Nevertheless, consumers clearly have already suffered significant and lasting harm as a result of the Data Breach, and such harm is likely to continue and worsen over time.

71. Armed with an individual's sensitive and personal information—including in particular a social security number, date of birth, and/or a drivers' license number—a criminal can commit identity theft, financial fraud, and other identity-related crimes. According to the Federal Trade Commission ("FTC"):

Once identity thieves have your personal information, they can drain your bank account, run up charges on your credit cards, open new utility accounts, or get medical treatment on your health insurance. An identity thief can file a tax refund in your name and get your refund. In some extreme cases, a thief might even give your name to the police during an arrest.<sup>2</sup>

72. Identity theft results in real financial losses, lost time, and aggravation to consumers. In its 2014 Victims of Identity Theft report, the United States Department of Justice stated that 65% of the over 17 million identity theft victims that year suffered a financial loss, and 13% of the total identity theft victims never had those losses reimbursed.<sup>3</sup> The average out-of-pocket loss for those victims was \$2,895. Identity theft victims also "paid higher interest rates on credit cards, they were turned down for loans or other credit, their utilities were turned off, or they were the subject of criminal proceedings."<sup>4</sup> With respect to consumers' emotional distress, the report also noted that more than one-third of identity theft victims were moderately or severely distressed due to the crime.<sup>5</sup>

73. The Data Breach has substantially increased the risk that the affected Massachusetts consumers will be a victim of identity theft or financial fraud at some unknown point in the future.

---

<sup>2</sup> See <https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft>.

<sup>3</sup> U.S. Dept. of Justice, Bureau of Justice Statistics, *Victims of Identity Theft 2014*, at 6 & Table 6, available at <http://www.bjs.gov/index.cfm?ty=pbdetail&iid=5408>.

<sup>4</sup> *Id.* at 8.

<sup>5</sup> See *id.* at 9, Table 9.



74. In order to protect themselves from this increased risk of identity theft and fraud, many consumers may place “security freezes” on their credit reports with one or more consumer reporting agency, including Equifax. The primary objective of a security freeze is to prevent third parties from accessing the frozen credit report when a new application for credit is placed without the consumer’s consent.

75. Massachusetts law permits, but does not require, the consumer reporting agency to charge the consumer a “reasonable fee, not to exceed \$5,” to place, lift, or remove a freeze on the consumer’s credit report. See G.L. c. 93, § 62A.

76. As a result of Equifax’s actions and inactions in connection with the Data Breach, and in an effort to protect themselves against identity theft or financial fraud, many Massachusetts consumers have already spent and will continue to spend time and money in an effort to place security freezes on their credit reports with Equifax and other consumer reporting agencies.

77. Further, Equifax has complicated consumers’ efforts to protect themselves from the harms caused by the Data Breach by failing to take various measures that it was uniquely positioned to take to mitigate the risk of harm caused by the Data Breach. Instead, Equifax has failed to clearly and promptly notify consumers whether they were affected by the Data Breach, has charged consumers to place security freezes (and presumably unfairly profited thereby), has failed to offer consumers free credit and fraud monitoring beyond one year, and has failed to ensure adequate call center staffing and availability of online services in the days following the September 7, 2017 announcement of the Data Breach. Equifax’s actions and inactions in this regard have compounded the harms already suffered by consumers.

**CAUSES OF ACTION**

**COUNT I**

**Violations of G.L. c. 93H, § 3 – Failure to Give Prompt Notice of Data Breach**

78. The Commonwealth incorporates and realleges herein the allegations in paragraphs 1–77.

79. The Commonwealth “may bring an action pursuant to section 4 of chapter 93A against a person or otherwise to remedy violations of [c. 93H] and for other relief that may be appropriate.” G.L. c. 93H, § 6.

80. As a corporation, Equifax is a “person” under G.L. c. 93H, § 1(a).

81. General Laws c. 93H, § 3(b) requires that a person who:

[O]wns or licenses data that includes personal information about a resident of the commonwealth, shall provide notice, as soon as practicable and without unreasonable delay, when such person or agency (1) knows or has reason to know of a breach of security or (2) when the person or agency knows or has reason to know that the personal information of such resident was acquired or used by an unauthorized person or used for an unauthorized purpose, to the attorney general, the director of consumer affairs and business regulation and to such resident in accordance with this chapter.

82. “Personal Information” is defined in G.L. c. 93H, § 1(a) as:

[A] [Massachusetts] resident’s first name and last name or first initial and last name in combination with any 1 or more of the following data elements that relate to such resident: (a) Social Security number; (b) driver’s license number or state-issued identification card number; or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident’s financial account . . . .

83. At all relevant times, Equifax owned or licensed personal information of at least one Massachusetts resident, as the term “personal information” is defined in G.L. c. 93H, § 1(a).

84. As of or soon after July 29, 2017, Equifax knew or should have known that the “personal information” (as defined in G.L. c. 93H, § 1(a)) of at least one Massachusetts resident

was acquired by an unauthorized person, and/or that the Data Breach was a “breach of security” as defined in G.L. c. 93H, § 1(a).

85. As of or soon after July 29, 2017, Equifax knew or should have known that it met the threshold for being able to provide “substitute notice” to Massachusetts residents as defined in G.L. 93H, § 1(a).

86. Equifax did not provide notice to the Attorney General, the Office of Consumer Affairs and Business Regulation, and affected consumers until September 7, 2017.

87. By not providing notice, substitute or otherwise, “as soon as practicable and without unreasonable delay” to the Attorney General, the Office of Consumer Affairs and Business Regulation, and affected consumers, Equifax violated G.L. c. 93H, § 3(b).

88. Each failure to notify each affected Massachusetts consumer, the Attorney General, and the Office of Consumer Affairs and Business Regulation constitutes a separate violation of G.L. c. 93H.

## **COUNT II**

### **Violations of G.L. c. 93H/201 CMR 17.00–17.05 – Failure to Safeguard Personal Information**

89. The Commonwealth hereby incorporates and realleges the allegations in paragraphs 1–88.

90. The Commonwealth “may bring an action pursuant to section 4 of chapter 93A against a person or otherwise to remedy violations of [c. 93H] and for other relief that may be appropriate.” G.L. c. 93H, § 6.

91. The Data Security Regulations, 201 CMR 17.00-17.05, were promulgated under authority of G.L. c. 93H, § 2.

92. The Data Security Regulations “apply to all persons that own or license personal information about a resident of the Commonwealth.” 201 CMR 17.01(2).

93. As a corporation, Equifax is a “person” under the Data Security Regulations. See 201 CMR 17.02.

94. The definition of “Personal Information” in the Data Security Regulations is coextensive to the definition of “Personal Information” in G.L. c. 93H, § 1, which is set forth in paragraph 82. See 201 CMR 17.02.

95. An entity “owns or licenses” personal information under the Data Security Regulations if it “receives, stores, maintains, processes, or otherwise has access to personal information in connection with the provision of goods or services or in connection with employment.” 201 CMR 17.02.

96. Equifax is bound by the Data Security Regulations because at all relevant times, it owned or licensed personal information of at least one Massachusetts resident and continues to own or license the personal information of Massachusetts residents.

97. The Data Security Regulations “establish[] minimum standards to be met in the connection with the safeguarding of personal information contained in both paper and electronic records.” 201 CMR 17.01(1).

98. Among these minimum standards is the duty of “[e]very person that owns or licenses personal information about a resident of the Commonwealth” to “develop, implement, and maintain” a written information security program (a “WISP”) that “contains administrative, technical, and physical safeguards that are appropriate to (a) the size, scope and type of business . . . ; (b) the amount of resources available to such person; (c) the amount of stored data; and

(d) the need for security and confidentiality of both consumer and employee information.” 201 CMR 17.03(1).

99. The Data Security Regulations mandate certain minimum safeguards and obligations that an entity must develop, implement, and maintain in its WISP, including among others:

- To “[i]dentify[] and assess[] reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic . . . records containing personal information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks[.]” (201 CMR 17.03(2)(b));
- “[M]eans for detecting and preventing security system failures.” (201 CMR 17.03(2)(b)(3)); and
- “Regular monitoring to ensure that the comprehensive information security program is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of personal information; and upgrading information safeguards as necessary to limit risks.” (201 CMR 17.03(2)(h)).

100. The WISP must also include the “the establishment and maintenance of a security system covering its computers, including any wireless system, that, at a minimum, and to the extent technically feasible,” contains certain minimum elements, including:

- “Secure user authentication protocols including . . . (a) control of user IDs and other identifiers; (b) a reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices; (c) control of data security passwords to ensure that such passwords are kept in a location and/or format that does not compromise the security of the data they protect; (d) restricting access to active users and active user accounts only; and (e) blocking access to user identification after multiple unsuccessful attempts to gain access or the limitation placed on access for the particular system[.]” (201 CMR 17.04(1));
- “[S]ecure access control measures” over computer systems that “restrict access to records and files containing personal information to those who need such information to perform their job duties . . . .” (201 CMR 17.04(2)(a));
- “[S]ecure access control measures” over computer systems that “(b) assign unique identifications plus passwords, which are not vendor supplied default passwords, to each person with computer access, that are reasonably designed to maintain the integrity of the security of the access controls[.]” (201 CMR 17.04(2)(b));

- “Encryption of all transmitted records and files containing personal information that will travel across public networks, and encryption of all data containing personal information to be transmitted wirelessly.” (201 CMR 17.04(3));
- “Reasonable monitoring of systems, for unauthorized use of or access to personal information[.]” (201 CMR 17.04(4));
- “For files containing personal information on a system that is connected to the Internet, . . . reasonably up-to-date firewall protection and operating system security patches, reasonably designed to maintain the integrity of the personal information[.]” (201 CMR 17.04(6)); and
- “Reasonably up-to-date versions of system security agent software which must include malware protection and reasonably up-to-date patches and virus definitions, or a version of such software that can still be supported with up-to-date patches and virus definitions, and is set to receive the most current security updates on a regular basis.” (201 CMR 17.04(7)).

101. Equifax failed to develop, implement, and maintain its WISP and a security system covering its computers in such a way as to meet the minimum requirements of 201 CMR 17.03 and 201 CMR 17.04, including without limitation the minimum requirements set forth in 201 CMR 17.03(2)(b), (2)(b)(3), or (2)(h)); or 201 CMR 17.04(1), (2)(a), (2)(b), (3), (4), (6), or (7).

102. Equifax also failed to satisfy its obligations to develop, implement, and maintain a WISP that contained “administrative, technical, and physical safeguards that are appropriate” to: (a) “the size, scope and type of business of” Equifax; (b) “the amount of resources available to” Equifax; (c) the amount of data Equifax stores; and (d) “the need for security and confidentiality of both consumer and employee information.” 201 CMR 17.03(1).

103. These failures include, without limitation: not adequately patching or implementing other safeguards sufficient to avoid the March Security Vulnerability; keeping the Exposed Information unencrypted or otherwise not protected through other methods from unauthorized disclosure in an area of its network accessible to the Internet; and not maintaining multiple layers of security sufficient to protect personal information from compromise.

104. Each violation of the Data Security Regulations as to each affected Massachusetts resident is a separate violation of c. 93H, § 2.

105. Accordingly, Equifax violated G.L. c. 93H, § 2.

### **COUNT III**

#### **Violations of G.L. c. 93A, § 2 – Unfair Acts or Practices**

106. The Commonwealth hereby incorporates and realleges the allegations in paragraphs 1–105.

107. General Laws c. 93A, § 2(a) declares unlawful “unfair or deceptive acts or practices in the conduct of trade or commerce[.]”

108. Equifax conducts trade and commerce in Massachusetts and with Massachusetts consumers.

109. As a corporation, Equifax is a “person” under G.L. c. 93A, § 1(a).

110. Equifax has engaged in unfair or deceptive acts or practices in violation of G.L. c. 93A § 2(a).

111. Equifax’s unfair or deceptive acts or practices include: (a) failing to promptly notify the public (including the Attorney General’s Office and affected residents) of the Data Breach despite the existence of substantial risk to consumers from the Data Breach; and/or (b) failing to maintain reasonable safeguards sufficient to secure the private and sensitive information about Massachusetts consumers from known and foreseeable threats of unauthorized access or unauthorized use, including identity theft, financial fraud, or other harms.

112. In addition, each of Equifax's violations of G.L. c. 93H and 201 CMR 17.00–17.05, as alleged herein and in Counts I & II, *supra*, are unfair or deceptive acts or practices in violation of G.L. c. 93A, § 2(a).

113. Accordingly, Equifax violated G.L. c. 93A, § 2.

114. Each and every violation of G.L. c. 93H and 201 CMR 17.00–17.05 with respect to each Massachusetts consumer is a separate violation of G.L. c. 93A, § 2.

115. Equifax knew or should have known that each of its violations of G.L. c. 93H and 201 CMR 17.00–17.05, each failure to maintain reasonable safeguards to protect Massachusetts consumers' sensitive and personal information, and each failure to promptly notify the public of the Data Breach, would violate G.L. c. 93A, § 2.

116. Although consumer harm is not an element of a claim under c. 93A, § 4, each and every consumer affected by the Data Breach has suffered and/or will suffer financial losses, and the associated stress and anxiety, as a result of the above unfair or deceptive acts or practices, including without limitation the costs to place, lift, and/or terminate security freezes with all applicable consumer reporting bureaus, remedial measures to prevent or respond to identity theft or other fraud, and out of pocket losses resulting therefrom.

#### **COUNT IV**

##### **Violation of G.L. c. 93A, § 2 – Deceptive Acts or Practices**

117. The Commonwealth hereby incorporates and realleges the allegations in paragraphs 1–116.

118. At all relevant times, Equifax represented to the public on its online Privacy



Policy that it has:

[B]uilt our reputation on our commitment to deliver reliable information to our customers (both businesses and consumers) and to protect the privacy and confidentiality of personal information about consumers. We also protect the sensitive information we have about businesses. Safeguarding the privacy and security of information, both online and offline, is a top priority for Equifax.

119. In its “Consumer Privacy Policy for Personal Credit Reports,” accessible at <http://www.equifax.com/privacy/personal-credit-reports>, Equifax further publicly represented that it has “reasonable, physical, technical and procedural safeguards to help protect your [i.e. consumers’] personal information.”

120. Equifax’s failures: to patch or otherwise adequately address the March Security Vulnerability; detect the hackers in their network; prevent them from accessing and stealing the Exposed Information; and otherwise failing to safeguard the Exposed Information, as alleged in paragraphs 21 to 49, herein, rendered these representations deceptive.

121. Additionally, Equifax’s failure to implement, develop, and/or maintain a WISP compliant with the Data Security Regulations or industry standards, as alleged in paragraphs 50 to 61 and 89 to 105, herein, rendered these representations deceptive.

122. Equifax’s public representations of the nature of its security safeguards over Massachusetts consumers’ sensitive and personal information were unfair or deceptive under G.L. c. 93A, § 2(a).

123. Accordingly, Equifax violated G.L. c. 93A, § 2.

124. Equifax knew or should have known that its misrepresentations of the nature of its security safeguards over Massachusetts consumers’ sensitive and personal information would violate G.L. c. 93A, § 2.

COUNT V**Violation of G.L. c. 93A , § 2 – Unfair or Deceptive Trade Practices**

125. The Commonwealth hereby incorporates and realleges the allegations in paragraphs 1– 124.

126. Equifax committed unfair or deceptive acts or practices under G.L. c. 93A, § 2, by failing to adequately allow or otherwise hindering the ability of Massachusetts consumers to protect themselves from harm resulting from the Data Breach by failing to make sufficiently available measures that Equifax was uniquely positioned to provide to mitigate the public harm caused by the Data Breach, namely:

- Timely notice of the Data Breach;
- Free security freezes of Equifax credit reports;
- Free Credit and fraud monitoring of Equifax credit reports for more than one year;
- Ensuring adequate and competent call center staffing related to the Data Breach;
- and
- Ensuring the availability of online services that notified consumers of whether they were affected by the Data Breach and allowed consumers to place a security freeze.

127. Accordingly, Equifax violated G.L. c. 93A, § 2.

128. Equifax knew or should have known that that the conduct described in paragraphs 69 to 77 and 125 to 126 would violate G.L. c. 93A, § 2.

**PRAYER FOR RELIEF**

WHEREFORE, the Commonwealth requests that the Court grant the following relief:

1. Enter a permanent injunction prescribing appropriate relief;
2. Order that Equifax pay civil penalties, restitution, and costs of investigation and litigation of this matter, including reasonable attorney's fees, to the Commonwealth of Massachusetts as provided for under G.L. c. 93A, § 4, in an amount to be determined at trial;
3. Disgorge profits Equifax obtained during or as a result of the Data Breach; and
4. Order such other just and proper legal and equitable relief.

**REQUEST FOR JURY TRIAL**


The Commonwealth hereby requests trial by jury as to all issues so triable.

Respectfully submitted,

COMMONWEALTH OF MASSACHUSETTS

MAURA HEALEY  
ATTORNEY GENERAL

By:

  
Sara Cable (BBO #667084)  
Jared Rinehimer (BBO #684701)  
Michael Lecaroz (BBO #672397)  
Assistant Attorneys General  
Consumer Protection Division  
One Ashburton Place, 18<sup>th</sup> Floor  
Boston, MA 02108  
(617) 727-2200  
sara.cable@state.ma.us  
jared.rinehimer@state.ma.us  
michael.lecaroz@state.ma.us

Date: *September 19, 2017*

## **Exhibit 2**



**PART I** ADMINISTRATION OF THE GOVERNMENT  
(Chapters 1 through 182)

**TITLE XV** REGULATION OF TRADE

**CHAPTER 93H** SECURITY BREACHES

**Section 1** Definitions

Section 1. (a) As used in this chapter, the following words shall, unless the context clearly requires otherwise, have the following meanings:—

“Agency”, any agency, executive office, department, board, commission, bureau, division or authority of the commonwealth, or any of its branches, or of any political subdivision thereof.

“Breach of security”, the unauthorized acquisition or unauthorized use of unencrypted data or, encrypted electronic data and the confidential process or key that is capable of compromising the security, confidentiality, or integrity of personal information, maintained by a person or agency that creates a substantial risk of identity theft or fraud against a resident of the commonwealth. A good faith but unauthorized acquisition of personal information by a person or agency, or employee or agent thereof, for the lawful purposes of such person or agency, is not a breach of security unless the personal information is used in an unauthorized manner or subject to further unauthorized disclosure.

“Data” any material upon which written, drawn, spoken, visual, or electromagnetic information or images are recorded or preserved, regardless of physical form or characteristics.

“Electronic”, relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic or similar capabilities.

“Encrypted” transformation of data through the use of a 128-bit or higher algorithmic process into a form in which there is a low probability of assigning meaning without use of a confidential process or key, unless further defined by regulation of the department of consumer affairs and business regulation.

“Notice” shall include:—

(i) written notice;

(ii) electronic notice, if notice provided is consistent with the provisions regarding electronic records and signatures set forth in § 7001 (c) of Title 15 of the United States Code; and chapter 110G; or

(iii) substitute notice, if the person or agency required to provide notice demonstrates that the cost of providing written notice will exceed \$250,000, or that the affected class of Massachusetts residents

to be notified exceeds 500,000 residents, or that the person or agency does not have sufficient contact information to provide notice.

"Person", a natural person, corporation, association, partnership or other legal entity.

"Personal information" a resident's first name and last name or first initial and last name in combination with any 1 or more of the following data elements that relate to such resident:

- (a) Social Security number;
- (b) driver's license number or state-issued identification card number; or
- (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account; provided, however, that "Personal information" shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.

"Substitute notice", shall consist of all of the following:—

- (i) electronic mail notice, if the person or agency has electronic mail addresses for the members of the affected class of Massachusetts residents;
  - (ii) clear and conspicuous posting of the notice on the home page of the person or agency if the person or agency maintains a website; and
  - (iii) publication in or broadcast through media or medium that provides notice throughout the commonwealth.
- (b) The department of consumer affairs and business regulation may adopt regulations, from time to time, to revise the definition of "encrypted", as used in this chapter, to reflect applicable technological advancements.



**PART I** ADMINISTRATION OF THE GOVERNMENT  
(Chapters 1 through 182)

**TITLE XV** REGULATION OF TRADE

**CHAPTER 93H** SECURITY BREACHES

**Section 2** Regulations to safeguard personal information of commonwealth residents

Section 2. (a) The department of consumer affairs and business regulation shall adopt regulations relative to any person that owns or licenses personal information about a resident of the commonwealth. Such regulations shall be designed to safeguard the personal information of residents of the commonwealth and shall be consistent with the safeguards for protection of personal information set forth in the federal regulations by which the person is regulated. The objectives of the regulations shall be to: insure the security and confidentiality of customer information in a manner fully consistent with industry standards; protect against anticipated threats or hazards to the security or integrity of such information; and protect against unauthorized access to or use of such information that may result in substantial harm or inconvenience to any consumer. The regulations shall take into account the person's size, scope and type of business, the amount of resources available to such person, the amount of stored data, and the need for security and confidentiality of both consumer and employee information.

(b) The supervisor of records, with the advice and consent of the information technology division to the extent of its jurisdiction to set information technology standards under paragraph (d) of section 4A of chapter 7, shall establish rules or regulations designed to safeguard the personal information of residents of the commonwealth that is owned or licensed. Such rules or regulations shall be applicable to: (1) executive offices and any agencies, departments, boards, commissions and instrumentalities within an executive office; and (2) any authority created by the General Court, and the rules and regulations shall take into account the size, scope and type of services provided thereby, the amount of resources available thereto, the amount of stored data, and the need for security and confidentiality of both consumer and employee information. The objectives of the rules or regulations shall be to: insure the security and confidentiality of personal information; protect against anticipated threats or hazards to the security or integrity of such information; and to protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any resident of the commonwealth.

(c) The legislative branch, the judicial branch, the attorney general, the state secretary, the state treasurer and the state auditor shall adopt rules or regulations designed to safeguard the personal information of residents of the commonwealth for their respective departments and shall take into account the size, scope and type of services provided by their departments, the amount of resources available thereto, the amount of stored data, and the need for security and confidentiality of both consumer and employee information. The objectives of the rules or regulations shall be to: insure the security and confidentiality of customer information in a manner fully consistent with

industry standards; protect against anticipated threats or hazards to the security or integrity of such information; and protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any resident of the commonwealth.



**PART I** ADMINISTRATION OF THE GOVERNMENT  
(Chapters 1 through 182)

**TITLE XV** REGULATION OF TRADE

**CHAPTER 93H** SECURITY BREACHES

**Section 3** Duty to report known security breach or unauthorized use of personal information

Section 3. (a) A person or agency that maintains or stores, but does not own or license data that includes personal information about a resident of the commonwealth, shall provide notice, as soon as practicable and without unreasonable delay, when such person or agency (1) knows or has reason to know of a breach of security or (2) when the person or agency knows or has reason to know that the personal information of such resident was acquired or used by an unauthorized person or used for an unauthorized purpose, to the owner or licensor in accordance with this chapter. In addition to providing notice as provided herein, such person or agency shall cooperate with the owner or licensor of such information. Such cooperation shall include, but not be limited to, informing the owner or licensor of the breach of security or unauthorized acquisition or use, the date or approximate date of such incident and the nature thereof, and any steps the person or agency has taken or plans to take relating to the incident, except that such cooperation shall not be deemed to require the disclosure of confidential business information or trade secrets, or to provide notice to a resident that may have been affected by the breach of security or unauthorized acquisition or use.

(b) A person or agency that owns or licenses data that includes personal information about a resident of the commonwealth, shall provide notice, as soon as practicable and without unreasonable delay, when such person or agency (1) knows or has reason to know of a breach of security or (2) when the person or agency knows or has reason to know that the personal information of such resident was acquired or used by an unauthorized person or used for an unauthorized purpose, to the attorney general, the director of consumer affairs and business regulation and to such resident, in accordance with this chapter. The notice to be provided to the attorney general and said director, and consumer reporting agencies or state agencies if any, shall include, but not be limited to, the nature of the breach of security or unauthorized acquisition or use, the number of residents of the commonwealth affected by such incident at the time of notification, and any steps the person or agency has taken or plans to take relating to the incident.

Upon receipt of this notice, the director of consumer affairs and business regulation shall identify any relevant consumer reporting agency or state agency, as deemed appropriate by said director, and forward the names of the identified consumer reporting agencies and state agencies to the notifying person or agency. Such person or agency shall, as soon as practicable and without unreasonable delay, also provide notice, in accordance with this chapter, to the consumer reporting agencies and state agencies identified by the director of consumer affairs and business regulation.

The notice to be provided to the resident shall include, but not be limited to, the consumer's right to obtain a police report, how a consumer requests a security freeze and the necessary information to

be provided when requesting the security freeze, and any fees required to be paid to any of the consumer reporting agencies, provided however, that said notification shall not include the nature of the breach or unauthorized acquisition or use or the number of residents of the commonwealth affected by said breach or unauthorized access or use.

(c) If an agency is within the executive department, it shall provide written notification of the nature and circumstances of the breach or unauthorized acquisition or use to the information technology division and the division of public records as soon as practicable and without unreasonable delay following the discovery of a breach of security or unauthorized acquisition or use, and shall comply with all policies and procedures adopted by that division pertaining to the reporting and investigation of such an incident.



**PART I** ADMINISTRATION OF THE GOVERNMENT  
(Chapters 1 through 182)

**TITLE XV** REGULATION OF TRADE

**CHAPTER 93H** SECURITY BREACHES

**Section 4** Delay in notice when notice would impede criminal investigation; cooperation with law enforcement

Section 4. Notwithstanding section 3, notice may be delayed if a law enforcement agency determines that provision of such notice may impede a criminal investigation and has notified the attorney general, in writing, thereof and informs the person or agency of such determination. If notice is delayed due to such determination and as soon as the law enforcement agency determines and informs the person or agency that notification no longer poses a risk of impeding an investigation, notice shall be provided, as soon as practicable and without unreasonable delay. The person or agency shall cooperate with law enforcement in its investigation of any breach of security or unauthorized acquisition or use, which shall include the sharing of information relevant to the incident; provided however, that such disclosure shall not require the disclosure of confidential business information or trade secrets.



**PART I** ADMINISTRATION OF THE GOVERNMENT  
(Chapters 1 through 182)

**TITLE XV** REGULATION OF TRADE

**CHAPTER 93H** SECURITY BREACHES

**Section 5** Applicability of other state and federal laws

Section 5. This chapter does not relieve a person or agency from the duty to comply with requirements of any applicable general or special law or federal law regarding the protection and privacy of personal information; provided however, a person who maintains procedures for responding to a breach of security pursuant to federal laws, rules, regulations, guidance, or guidelines, is deemed to be in compliance with this chapter if the person notifies affected Massachusetts residents in accordance with the maintained or required procedures when a breach occurs; provided further that the person also notifies the attorney general and the director of the office of consumer affairs and business regulation of the breach as soon as practicable and without unreasonable delay following the breach. The notice to be provided to the attorney general and the director of the office of consumer affairs and business regulation shall consist of, but not be limited to, any steps the person or agency has taken or plans to take relating to the breach pursuant to the applicable federal law, rule, regulation, guidance or guidelines; provided further that if said person or agency does not comply with applicable federal laws, rules, regulations, guidance or guidelines, then it shall be subject to the provisions of this chapter

**PART I** ADMINISTRATION OF THE GOVERNMENT  
(Chapters 1 through 182)

**TITLE XV** REGULATION OF TRADE

**CHAPTER 93H** SECURITY BREACHES

**Section 6** Enforcement of chapter

Section 6. The attorney general may bring an action pursuant to section 4 of chapter 93A against a person or otherwise to remedy violations of this chapter and for other relief that may be appropriate

## **Exhibit 3**



**PART I** ADMINISTRATION OF THE GOVERNMENT  
(Chapters 1 through 182)

**TITLE XV** REGULATION OF TRADE

**CHAPTER 93I** DISPOSITIONS AND DESTRUCTION OF RECORDS

**Section 1** Definitions

Section 1. As used in this chapter the following words shall, unless the context clearly requires otherwise, have the following meanings:

"Agency". any county, city, town, or constitutional office or any agency thereof, including but not limited to, any department, division, bureau, board, commission or committee thereof, or any authority created by the general court to serve a public purpose, having either statewide or local jurisdiction.

"Data subject", an individual to whom personal information refers.

"Person" a natural person, corporation, association, partnership or other legal entity.

"Personal information", a resident's first name and last name or first initial and last name in combination with any 1 or more of the following data elements that relate to the resident:—

- (a) Social Security number;
- (b) driver's license number or Massachusetts identification card number;
- (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password that would permit access to a resident's financial account; or
- (d) a biometric indicator.



**PART I** ADMINISTRATION OF THE GOVERNMENT  
(Chapters 1 through 182)

**TITLE XV** REGULATION OF TRADE

**CHAPTER 93I** DISPOSITIONS AND DESTRUCTION OF RECORDS

**Section 2** Standards for disposal of records containing personal information; disposal by third party; enforcement

Section 2. When disposing of records, each agency or person shall meet the following minimum standards for proper disposal of records containing personal information:

- (a) paper documents containing personal information shall be either redacted, burned, pulverized or shredded so that personal data cannot practicably be read or reconstructed;
- (b) electronic media and other non-paper media containing personal information shall be destroyed or erased so that personal information cannot practicably be read or reconstructed.

Any agency or person disposing of personal information may contract with a third party to dispose of personal information in accordance with this chapter. Any third party hired to dispose of material containing personal information shall implement and monitor compliance with policies and procedures that prohibit unauthorized access to or acquisition of or use of personal information during the collection, transportation and disposal of personal information.

Any agency or person who violates the provisions of this chapter shall be subject to a civil fine of not more than \$100 per data subject affected, provided said fine shall not exceed \$50,000 for each instance of improper disposal. The attorney general may file a civil action in the superior or district court in the name of the commonwealth to recover such penalties.



**PART I** ADMINISTRATION OF THE GOVERNMENT  
(Chapters 1 through 182)

**TITLE XV** REGULATION OF TRADE

**CHAPTER 93I** DISPOSITIONS AND DESTRUCTION OF RECORDS

**Section 3** Enforcement

Section 3. The attorney general may bring an action pursuant to section 4 of chapter 93A against a person or otherwise to remedy violations of this chapter and for other relief that may be appropriate.

## **Exhibit 4**

**201 CMR 17.00: STANDARDS FOR THE PROTECTION OF PERSONAL INFORMATION OF RESIDENTS OF THE COMMONWEALTH**

## Section:

17.01: Purpose and Scope

17.02: Definitions

17.03: Duty to Protect and Standards for Protecting Personal Information

17.04: Computer System Security Requirements

17.05: Compliance Deadline

**17.01 Purpose and Scope****(1) Purpose**

This regulation implements the provisions of M.G.L. c. 93H relative to the standards to be met by persons who own or license personal information about a resident of the Commonwealth of Massachusetts. This regulation establishes minimum standards to be met in connection with the safeguarding of personal information contained in both paper and electronic records. The objectives of this regulation are to insure the security and confidentiality of customer information in a manner fully consistent with industry standards; protect against anticipated threats or hazards to the security or integrity of such information; and protect against unauthorized access to or use of such information that may result in substantial harm or inconvenience to any consumer.

**(2) Scope**

The provisions of this regulation apply to all persons that own or license personal information about a resident of the Commonwealth.

**17.02: Definitions**

The following words as used herein shall, unless the context requires otherwise, have the following meanings:

**Breach of security**, the unauthorized acquisition or unauthorized use of unencrypted data or, encrypted electronic data and the confidential process or key that is capable of compromising the security, confidentiality, or integrity of personal information, maintained by a person or agency that creates a substantial risk of identity theft or fraud against a resident of the commonwealth. A good faith but unauthorized acquisition of personal information by a person or agency, or employee or agent thereof, for the lawful purposes of such person or agency, is not a breach of security unless the personal information is used in an unauthorized manner or subject to further unauthorized disclosure.

**Electronic**, relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic or similar capabilities.

**Encrypted**, the transformation of data into a form in which meaning cannot be assigned without the use of a confidential process or key.

**Owns or licenses**, receives, stores, maintains, processes, or otherwise has access to personal information in connection with the provision of goods or services or in connection with employment.

**Person**, a natural person, corporation, association, partnership or other legal entity, other than an agency, executive office, department, board, commission, bureau, division or authority of the Commonwealth, or any of its branches, or any political subdivision thereof.

**Personal information**, a Massachusetts resident's first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such resident: (a) Social Security number; (b) driver's license number or state-issued identification card number; or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account; provided, however, that "Personal information" shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.

**Record or Records**, any material upon which written, drawn, spoken, visual, or electromagnetic information or images are recorded or preserved, regardless of physical form or characteristics.

**Service provider**, any person that receives, stores, maintains, processes, or otherwise is permitted access to personal information through its provision of services directly to a person that is subject to this regulation.

#### **17.03: Duty to Protect and Standards for Protecting Personal Information**

(1) Every person that owns or licenses personal information about a resident of the Commonwealth shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to (a) the size, scope and type of business of the person obligated to safeguard the personal information under such comprehensive information security program; (b) the amount of resources available to such person; (c) the amount of stored data; and (d) the need for security and confidentiality of both consumer and employee information. The safeguards contained in such program must be consistent with the safeguards for protection of personal information and information of a similar character set forth in any state or federal regulations by which the person who owns or licenses such information may be regulated.

(2) Without limiting the generality of the foregoing, every comprehensive information security program shall include, but shall not be limited to:

- (a) Designating one or more employees to maintain the comprehensive information security program;
- (b) Identifying and assessing reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, including but not limited to:
  - 1. ongoing employee (including temporary and contract employee) training;
  - 2. employee compliance with policies and procedures; and
  - 3. means for detecting and preventing security system failures.
- (c) Developing security policies for employees relating to the storage, access and transportation of records containing personal information outside of business premises.
- (d) Imposing disciplinary measures for violations of the comprehensive information security program rules.
- (e) Preventing terminated employees from accessing records containing personal information.
- (f) Oversee service providers, by:
  - 1. Taking reasonable steps to select and retain third-party service providers that are capable of maintaining appropriate security measures to protect such personal information consistent with these regulations and any applicable federal regulations; and
  - 2. Requiring such third-party service providers by contract to implement and maintain such appropriate security measures for personal information; provided, however, that until March 1, 2012, a contract a person has entered into with a third party service provider to perform services for said person or functions on said person's behalf satisfies the provisions of 17.03(2)(f)(2) even if the contract does not include a requirement that the third party service provider maintain such appropriate safeguards, as long as said person entered into the contract no later than March 1, 2010.
- (g) Reasonable restrictions upon physical access to records containing personal information,, and storage of such records and data in locked facilities, storage areas or containers.
- (h) Regular monitoring to ensure that the comprehensive information security program is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of personal information; and upgrading information safeguards as necessary to limit risks.
- (i) Reviewing the scope of the security measures at least annually or whenever there is a material change in business practices that may reasonably implicate the security or integrity of records containing personal information.
- (j) Documenting responsive actions taken in connection with any incident involving a breach of security, and mandatory post-incident review of events and actions taken, if any, to make changes in business practices relating to protection of personal information.

#### **17.04: Computer System Security Requirements**

Every person that owns or licenses personal information about a resident of the Commonwealth and electronically stores or transmits such information shall include in its written, comprehensive information security program the establishment and maintenance of a

security system covering its computers, including any wireless system, that, at a minimum, and to the extent technically feasible, shall have the following elements:

- (1) Secure user authentication protocols including:
  - (a) control of user IDs and other identifiers;
  - (b) a reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices;
  - (c) control of data security passwords to ensure that such passwords are kept in a location and/or format that does not compromise the security of the data they protect;
  - (d) restricting access to active users and active user accounts only; and
  - (e) blocking access to user identification after multiple unsuccessful attempts to gain access or the limitation placed on access for the particular system;
- (2) Secure access control measures that:
  - (a) restrict access to records and files containing personal information to those who need such information to perform their job duties; and
  - (b) assign unique identifications plus passwords, which are not vendor supplied default passwords, to each person with computer access, that are reasonably designed to maintain the integrity of the security of the access controls;
- (3) Encryption of all transmitted records and files containing personal information that will travel across public networks, and encryption of all data containing personal information to be transmitted wirelessly.
- (4) Reasonable monitoring of systems, for unauthorized use of or access to personal information;
- (5) Encryption of all personal information stored on laptops or other portable devices;
- (6) For files containing personal information on a system that is connected to the Internet, there must be reasonably up-to-date firewall protection and operating system security patches, reasonably designed to maintain the integrity of the personal information.
- (7) Reasonably up-to-date versions of system security agent software which must include malware protection and reasonably up-to-date patches and virus definitions, or a version of such software that can still be supported with up-to-date patches and virus definitions, and is set to receive the most current security updates on a regular basis.
- (8) Education and training of employees on the proper use of the computer security system and the importance of personal information security.

**17.05: Compliance Deadline**

- (1) Every person who owns or licenses personal information about a resident of the Commonwealth shall be in full compliance with 201 CMR 17.00 on or before March 1, 2010.

**REGULATORY AUTHORITY**

201 CMR 17.00: M.G.L. c. 93H

## **EXHIBIT 5**



MAGNA HALL  
ATTORNEY GENERAL

THE COMMONWEALTH OF MASSACHUSETTS  
OFFICE OF THE ATTORNEY GENERAL

ONE ASHBURTON PLACE  
BOSTON, MASSACHUSETTS 02108

TEL: (617) 725-2200  
WWW.BAGS.GOV.CM

March 17, 2015

The Honorable Michael C. Burgess M.D.  
Chairman  
Subcommittee on Commerce,  
Manufacturing, & Trade  
Energy and Commerce Committee  
U.S. House of Representatives  
Washington, DC 20215

The Honorable Jan Schakowsky  
Ranking Member  
Subcommittee on Commerce,  
Manufacturing, & Trade  
Energy and Commerce Committee  
U.S. House of Representatives  
Washington, DC 20215

Re: *The Data Security and Breach Notification Act of 2015*

Dear Chairman Burgess and Ranking Member Schakowsky:

We write to address the discussion draft bill entitled the Data Security and Breach Notification Act of 2015 (the "Bill"), dated March 12, 2015, which seeks to establish federal standards concerning data security and data breach notification obligations. We appreciate that the Committee recognizes the importance of strong data security protections and breach disclosure obligations to protect consumers and preserve consumer confidence in the market. Moreover, we are cognizant of the business community's concerns regarding compliance with myriad state security breach notification regimes.

Nonetheless, we write to express serious reservations with the Bill, which in our view represents an unnecessary retraction of existing protections for consumers at a time when such protections are imperative. Our concerns are informed by this Office's experience enforcing Massachusetts' data security breach notification law (Mass. Gen. Law ch. 93H, attached as Exhibit 1), data security regulations (Title 201 of the Code of Massachusetts Regulations ("CMR"), section 17.00 *et seq.*, attached as Exhibit 2), and data disposal law (Mass. Gen. Law ch. 93I, attached as Exhibit 3). Together, these laws and regulations – which are enforced by this Office through the Massachusetts Consumer Protection Act<sup>1</sup> – require entities that own or license "personal information"<sup>2</sup> of Massachusetts residents to develop, implement, and maintain

<sup>1</sup> Mass Gen. Law ch. 93A.

<sup>2</sup> In Massachusetts, "personal information" is defined by statute to mean a resident's first name and last name, or first initial and last name, in combination with any one or more of the following data elements: (a) social security



minimum security procedures and policies consistent with industry standards to safeguard such information (whether in paper or electronic form) from anticipated threats or hazards and from unauthorized access or use.<sup>3</sup> Massachusetts law also obligates entities to provide prompt notice to affected residents and state agencies in the event of a breach of security or compromise of that information.<sup>4</sup> These laws and regulations protect consumers from identity theft and fraud, and concomitantly, instill consumer confidence in the commercial collection and use of their personal information.

From January 1, 2008 through July 31, 2014, this Office received notice pursuant to Mass. Gen. Law ch. 93H, section 3 of over 8,665 security breaches, affecting nearly 5 million Massachusetts residents. To the extent any of those breaches resulted in enforcement actions by this Office (a very small percentage), the circumstances reflected gross failures to implement or maintain basic security practices, unreasonable delays in providing notice of the breach, or other egregious conduct that raised real risks of resulting consumer harm. As a result, this Office has an informed and comprehensive view into the nature, extent, and frequency of data breaches, the risks faced by consumers, and the security practices and procedures that can prevent or mitigate those risks.

Accordingly, this Office is uniquely positioned to highlight some of the potential problems with the Bill. Our principal concerns are as follows:

**I. The Bill's proposed preemption of state law undercuts existing consumer protections and is overly broad.**

Although the stated purpose of the Bill is to "protect consumers from identity theft, economic loss or economic harm, and financial fraud," the Bill would preempt Massachusetts' data security/breach law to the extent they relate to data in electronic form, and replace it with weaker protections. In addition, the Bill would preempt other state laws that protect "data in electronic form" from unauthorized access (including, among others, laws that criminalize the interception of wire communications (Mass Gen. Law c. 272, § 99(C)) or require the confidentiality of medical records and mental health records (Mass Gen. Law c. 111, § 70E(b), and c. 123, § 36)). It is also in conflict with, and would appear to potentially preempt, the enforcement authority given to the States under other federal laws relating to the security of electronic data (including, for example, the Health Information Technology for Economic and Clinical Health (HITECH) Act (42 U.S.C. 1320d-5(d))). Such sweeping preemption is harmful to consumers, and restricts innovative States from responding to and protecting their residents from emerging threats to the privacy and security of their data. The Bill should at least preserve the current level of protections enjoyed by consumers and the enforcement powers of the state Attorneys General to avoid a national downward harmonization of security and breach standards, and an associated drop in consumer confidence in the marketplace. The Bill will not only fail to

---

number; or (b) driver's license number or state-issued identification card number; or (c) financial account number or credit or debit card number, with or without any required security code. See Mass Gen. Law ch. 93H, §1.

<sup>3</sup> See Mass Gen. Law ch. 93I and 201 CMR 17.00 *et seq.*

<sup>4</sup> See Mass Gen. Law ch. 93H.

maintain consumer confidence in the marketplace, but will scale back the protections consumers currently enjoy.

**II. Minimum data security standards are important and necessary, but the proposed standards leave consumers' data vulnerable.**

We agree that establishing minimum data security standards is important and necessary. Massachusetts has had robust minimum data security regulations in place since 2010 in the form of data security regulations (201 CMR 17.00 *et seq.*) and data disposal law (Mass Gen. Law ch. 93I). The flexible standards established by Massachusetts represent the leading information security framework in the nation, and are the standards to which all commercial entities aspire.<sup>5</sup> We are concerned the Bill will lower the bar already set by Massachusetts and other existing federal data security regulations,<sup>6</sup> and will weaken consumers' confidence in the security of their personal information in commerce. Specifically, the Bill fails to articulate the minimum data security standards that would constitute the required "reasonable security measures and practices." As a result, the Bill would result in the retroactive establishment of data security standards through protracted litigation and piecemeal judicial interpretation. To ensure that the data security obligations are sufficiently robust, defined, and responsive to changing threats and technologies, the Bill should establish minimum data security standards, modeled after those in place in Massachusetts and under existing federal law.

**III. The Bill fails to require notice that will ensure meaningful enforcement.**

While the Bill's requirement of notice of a breach to the Federal Trade Commission is an important first step for enforcement of the Bill's requirements, it is not by itself enough. Recent breaches reported in the media underscore the necessary role played by the state Attorneys General in enforcing data breach and data security requirements. The absence of a requirement to provide notice to state Attorneys General of data breaches – even for those breaches that impact a significant number of their residents – frustrates their ability to protect their residents. Further, the threshold for providing notice to the FTC may be set too high. In Massachusetts, the vast majority (approximately 97%) of the 2,314 data breaches reported in 2013 involved fewer than 10,000 persons; each of these breaches affected, on average, 74 persons. Assuming these statistics are consistent nationally, the Bill would create an enforcement "blind spot" for both

<sup>5</sup> Similar to existing federal standards applicable to financial institutions (see 16 C.F.R. Part 314) and entities covered under HIPAA (see e.g. 45 CFR Subpart C of Part 164), Massachusetts requires entities to identify and assess reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of personal information (201 CMR 17.03(2)(b)); develop, implement and maintain a "written comprehensive information security program" containing physical, administrative and technical safeguards necessary to protect personal information from those risks (201 CMR 17.03); take reasonable steps to oversee third parties handling personal information (201 CMR 17.03(2)(f)); and securely dispose of personal information (Mass Gen. Law ch. 93I). Cognizant of the particular risks associated with electronic data, Massachusetts also requires entities, among other things, to establish and maintain a technically-feasible computer security system (201 CMR 17.04); and to encrypt personal information sent over public networks or wirelessly, or stored on laptops and portable devices (201 CMR 17.04(3), (5)).

<sup>6</sup> See, e.g., 16 C.F.R. Part 314 (Standards for Safeguarding Customer Information); 45 CFR Subpart C of Part 164 (Security Standards for the Protection of Electronic Protected Health Information); 16 CFR Part 682 (Proper Disposal of Consumer Information); and 201 CMR 17.00 *et seq.* (Standards for the Protection of Personal Information of Residents of the Commonwealth).

state and federal regulators, who would not receive notice of the vast majority of data breaches that occur. To ensure effective enforcement of the Bill, the Bill should require prompt notice of breaches to the FTC and also to the state Attorneys General in cases where their State's residents are impacted.

**IV. The Bill infringes on the States' consumer protection enforcement authority.**

While the Bill gives the state Attorneys General the option of bringing a civil action as *parens patriae* in U.S. district court, it requires the State to first notify the FTC, and to abstain from that action if the FTC initiates the action first. Such requirements infringe on the enforcement prerogatives of the state Attorneys General by injecting unnecessary delay and costs, and unnecessarily complicating their efforts to enforce their respective consumer protection laws. Numerous federal laws illustrate that dual federal/state enforcement coordination of consumer protection laws is both possible and effective, including for example: the Federal Trade Commission Act (15 U.S.C. § 45(a)(1) and its numerous State counterparts (see, e.g. Mass Gen. Law ch. 93A), the Fair Credit Reporting Act (15 U.S.C. § 1681 *et seq.*), the Health Insurance Portability and Accountability Act (HIPAA) (Pub. L. No. 104-191, 110 Stat. 1936 (1996)) and the Health Information Technology for Clinical and Economic Health (HITECH) Act (42 U.S.C. § 17930 *et seq.*). To ensure meaningful protections for consumers, the Bill should likewise establish a dual federal/state enforcement framework that respects – not constricts – the enforcement prerogative of the States.

**V. The penalties proposed by the Bill are insufficient, and leave consumers without a remedy.**

The Bill limits the state Attorneys General to civil penalties of up to \$11,000 for each day per violation of the Bill's information security requirements, and up to \$11,000 per violation of the Bill's breach notice requirements, capped at a total liability of \$2.5 million, and based on "penalty factors" that do not expressly take into account consumer harm or the need to deter future violations. Given the massive scope of recently-reported breaches affecting some of the largest companies in the country, a civil penalty cap of \$2.5 million may be an insufficient deterrent, and could be treated as a cost of doing business. Moreover, the Bill does not authorize the state Attorneys General to recover consumer restitution, and further does not provide for a private cause of action. Thus, a consumer who suffers loss due to a data breach effectively has no remedy under this Bill. The Bill should instead retain the existing discretion of state Attorneys General and the FTC to seek both civil penalties and consumer restitution at levels sufficient to penalize and deter the conduct at issue and make consumers whole, and further provide a private right of action.

**VI. The Bill's data breach notice obligations lack many key safeguards.**

Requiring prompt notice to consumers affected by a breach and to state regulators serves important ends, including alerting consumers to the fact that their personal information may be at risk, educating the market as to existing or emerging security threats, and providing incentives for improving security practices to prevent breaches. The data breach notice standards proposed by the Bill fall short for a number of reasons.

First, the Bill allows entities to delay notice without regard to the risks faced by consumers. By requiring notice only when the entity both “discovers” a “breach of security” and “determines” that a “reasonable risk of” identity theft, economic loss or harm, or financial fraud has resulted or will result, the Bill creates a disincentive for an entity to monitor their systems for potential compromises or vulnerabilities, an outcome directly at odds with the Bill’s stated purposes. Once “discovered,” the Bill would further grant a covered entity an unspecified (and unlimited) period of time to “tak[e] the necessary measures” to “determine the scope of the breach of security and restore the reasonable integrity, security, and confidentiality” of its data system. This creates opportunities for delay that would undermine the force of the proposed thirty (30) day notification deadline, and which may subject consumers to unnecessary risk. If preventing identity theft is the goal, notice should be issued in time for consumers to protect themselves, even if the breached entity has not completed its investigation or is still in the process of restoring its systems.

Second, the Bill fails to require notice in cases where identity theft is a real risk, such as when personal information is accessed or acquired with authorization (e.g. by an authorized employee) but used for unauthorized purposes. Additionally, the Bill does not provide for notice in cases where encrypted personal information – and information allowing for the decryption of that information – are both compromised in the breach.

Third, because notice obligation under the Bill turns on the manner in which a covered entity deals with the personal information, rather than its legal relationship to it,<sup>7</sup> notice could be delayed or avoided as a result of disputes between covered entities as to which is the “third-party entity” and which is the covered entity responsible for notice. It may also result in consumer confusion insofar as consumers may receive notice from an entity with which they have not had direct dealings. To avoid such results, the Bill should follow Massachusetts’ lead and impose the consumer notification duty on the entity that “owns or licenses” the breached personal information. In turn, entities that “maintain or store” the breached personal information should be obligated to promptly notify the owner or licensor. *See* Mass Gen. Law ch. 93H, §§ 3(a), (b).

Finally, the content and form of the required consumer notice lacks several key safeguards. The Bill does not require the notice to contain information as to how a consumer may protect him or herself and instead, directs the consumer to the FTC for more information. The Bill should require the consumer notice to contain the information necessary for the consumer to protect him/herself from identity theft.<sup>8</sup> In cases where “substitute notice” is

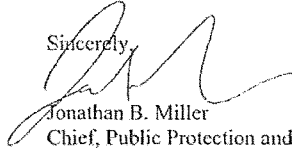
<sup>7</sup> The Bill imposes the consumer notice obligation on “a covered entity that uses, accesses, transmits, stores, disposes of, or collects” personal information (section 3(a)(1)), but not on the covered entity that “store[s], processe[s], or maintain[s]” personal information” for a covered entity. This “third-party entity” would “ha[ve] no other notification obligations” than to notify the covered entity for whom it stores, processes, or maintains the personal information (section 3(b)(1)(A)).

<sup>8</sup> Such information should include, for example, information concerning the availability of security freezes, the importance of filing and obtaining a police report (information required under Mass Gen. Law ch. 93H, § 3), the availability of fraud alerts, the importance of monitoring one’s credit reports, and other information about the breach that would allow the consumer to fairly assess their risk and protect themselves.

authorized, the entity should be required to make a media posting sufficient to constitute legal notice of the breach.<sup>9</sup>

We appreciate this opportunity to convey our serious concerns regarding the Bill to the Subcommittee. Please do not hesitate to contact us for any additional detail, clarity or with questions you may have. We are happy to provide you with any information you may need or to share with you our experience gained from working with businesses, reviewing security breach notifications, and enforcing our laws.

Sincerely,



Jonathan B. Miller  
Chief, Public Protection and Advocacy Bureau

Sara Cable  
Assistant Attorney General  
Consumer Protection Division

Office of Attorney General Maura Healey  
Commonwealth of Massachusetts  
One Ashburton Place  
Boston, MA 02108  
(617) 727-2200

<sup>9</sup> See, e.g. Mass Gen. Law ch. 93H, § 1 (requiring as one component of substitute notice "publication in or broadcast through media or medium that provides notice throughout the commonwealth [of Massachusetts]").



**Written Testimony of Mike Litt  
Consumer Advocate, U.S. PIRG**

**Continuation of Hearing entitled "Examining the Equifax Data  
Breach"**

**Before the Financial Services Committee  
United States House of Representatives**

**The Honorable Jeb Hensarling, Chairman  
The Honorable Maxine Waters, Ranking Member**

**October 25, 2017**

Chairman Hensarling, Ranking Member Waters, and Members of the Committee:

Thank you for the opportunity to testify on the best steps forward with the Equifax breach. I am the national consumer advocate for the U.S. Public Interest Research Group (U.S. PIRG). We are an independent non-profit group that promotes consumer rights. I work on identity theft prevention, among other consumer issues. In 2015, I wrote a report called, "Why You Should Get Security Freezes Before Your Information is Stolen."<sup>1</sup>

In my testimony today, I will outline how the products and services offered by Equifax after its data breach are failing to fully protect consumers. I will also discuss why consumers need credit freezes at all the big three credit bureaus and what type of legislation we need to facilitate more consumers getting those freezes.

## **I. Why Consumers Need Freezes at All the Big Three Credit Bureaus**

The Equifax breach is bad in many ways and has raised a lot of troubling questions. The question I'd like to focus on is why Equifax still has not provided or even clearly explained to consumers what they need to fully protect themselves.

There are different types of ID theft that can be committed depending on the type of information that has been stolen.

When credit card numbers are stolen, as they were for about 209,000 consumers in the Equifax breach<sup>2</sup>, an ID thief can rack up debt on existing credit card accounts.

When full names, birthdates and social security numbers are stolen, like they were for over 145 million Americans in the Equifax breach,<sup>3</sup> a few different types of ID theft can be committed, including new account fraud, tax refund fraud and medical services fraud.

Of all the possible types of ID theft out there, once your information has been stolen, there is only one kind that can be stopped before it happens. And that's where somebody opens a new credit account in your name - again, known as new account fraud - and racks up a ton of debt. The only way to prevent that is by getting credit freezes, also known as security freezes, at all three big national credit bureaus.

Credit freezes block potential creditors like a credit card company, cell phone store, or lender from viewing your credit report, which shows your credit history. And if they can't see that, they're just

<sup>1</sup> Ed Mierzwinski and Mike Litt, U.S. PIRG, *Why You Should Get Credit Freezes Before Your Information is Stolen*, October 2015.

<sup>2</sup> Equifax, *Equifax Announces Cybersecurity Incident Involving Consumer Information*, accessed at <https://www.equifaxsecurity2017.com/2017/09/07/equifax-announces-cybersecurity-incident-involving-consumer-information/>, 23 October 2017.

<sup>3</sup> Stacy Cowley, "2.5 Million More People Potentially Exposed in Equifax Breach," *The New York Times*, 2 October 2017.

not going open an account.<sup>4</sup> That's how you shut the door on identity thieves opening accounts in your name. And because creditors run checks with any one or a combination of the credit bureaus, you need to block access to your reports with all three bureaus. When you want to apply for credit, a loan, or insurance (or jobs that run credit checks), you can simply lift the freeze or temporarily "thaw" your report.

Disappointingly, Equifax has not adequately explained the need to block access to your credit report with all three credit bureaus.

## II. The Limitations of Equifax's TrustedID Premier Product

Equifax is offering a free product called TrustedID Premier, made up of five different services for one year, to anyone, whether their info was lost or not.<sup>5</sup> This package falls short of protecting consumers. Here's what they are offering and what the limitations of each are:

### 1. Copy of your Equifax Credit Report.

Looking at your credit report is a good idea because you can spot unauthorized credit accounts in your name. It's a good idea to check your credit report at all three bureaus, not just at Equifax. You can request free copies of your credit report at all three bureaus at [annualcreditreport.com](https://annualcreditreport.com), the official website authorized by the government for requesting these free reports.<sup>6,7</sup>

### 2. 3 Bureau Credit File Monitoring

TrustedID Premier includes credit monitoring at all three bureaus. Equifax should make it clear that monitoring only detects changes to your credit report. It does not detect fraudulent use of existing credit cards or any other type of fraudulent activity. And it does not actually prevent any kind of ID theft at all.

At best, monitoring will alert you to an ID thief opening an account in your name after they have already tried or successfully done so.

Due to huge marketing pushes by credit monitoring services and poor education by companies and other organizations after their data breaches, most consumers have not understood what they're getting with credit monitoring or that freezes are their only option for preventing any kind of ID theft.

<sup>4</sup> We are unaware of any firm that opens new accounts without a credit report or credit score.

<sup>5</sup> Equifax, *Equifax Announces Cybersecurity Incident Involving Consumer Information*, accessed at <https://www.equifaxsecurity2017.com/2017/09/07/equifax-announces-cybersecurity-incident-involving-consumer-information/>, 23 October 2017.

<sup>6</sup> The ability to request a free annual credit report from each of the three big credit bureaus comes from the Fair and Accurate Credit Transactions Act of 2003 (FACTA). This act amended the Fair Credit Reporting Act (FCRA), in order "to prevent identity theft, improve resolution of consumer disputes, improve the accuracy of consumer records, make improvements in the use of, and consumer access to, credit information, and for other purposes." See 108th Congress, *Fair and Accurate Credit Transactions Act of 2003*, 4 December 2003.

<sup>7</sup> The FTC has a page that explains how to access free credit reports by phone or regular mail too. See Federal Trade Commission, *Free Credit Reports*, accessed at <https://www.consumer.ftc.gov/articles/0155-free-credit-reports>, 23 October 2017.



They often also do not understand that “free trials” for subscription monitoring products quickly result in \$10-20/month bills. The Consumer Financial Protection Bureau in January took action against deceptive practices in the marketing of such products by both Equifax and Transunion.<sup>8</sup>

If you freeze your credit reports at all three credit bureaus and request a free copy of your credit report through [annualcreditreport.com](http://annualcreditreport.com) every 3-4 months, you don't really need credit monitoring. However, for consumers who don't get credit freezes, free monitoring of reports at all three credit bureaus should be available indefinitely, not just one year. The information that was stolen, including social security numbers and birthdates, does not have a shelf life.

### 3. Equifax Credit Report Lock

TrustedID Premier includes something similar to a credit freeze, something Equifax calls a “credit report lock,” but only for Equifax reports. The next section of this written testimony discusses concerns with locks in more detail.

Free freezes are not part of the TrustedID Premier product, but after public pressure, Equifax temporarily waived the fee for getting credit freezes through next January, but only for Equifax reports. The fee should be waived indefinitely, and free freezes should be offered for reports with all three credit bureaus.

Equifax is also reimbursing consumers who paid for a freeze for their Equifax report since September 7<sup>th</sup>. But Equifax should reimburse consumers who paid for freezes with the other bureaus too, not just with Equifax.

Identity thieves could still try to open credit accounts with companies that use the other two credit bureaus for credit checks. Therefore, a freeze or “lock” with only one bureau is incomplete protection.

### 4. Social Security Number Monitoring

Equifax advertises this services as searching “suspicious websites for your Social Security number.”<sup>9</sup> This service wouldn't hurt, but again, the only fraud that can actually be prevented once someone has your Social Security number is new account identity fraud. And the only way to prevent that is through credit freezes. You're best off getting credit freezes with all three bureaus.

### 5. \$1M Identity Theft Insurance

This is a feature that reimburses you for costs incurred from identity theft. It's worth noting that you might already have some sort of insurance or equivalent protection from fraud resulting from ID theft that is extended to you voluntarily by your employer, your insurance company (as a rider on your existing homeowner's or renter's insurance), or your credit card issuer (as a perk), etc. It's also important to point out that ID theft insurance, whether offered free or as part of a service that you're paying for always has limitations, exclusions, and requirements and usually only covers incidental

<sup>8</sup> Consumer Financial Protection Bureau, *CFPB Orders TransUnion and Equifax to Pay for Deceiving Consumers in Marketing Credit Scores and Credit Products*, 3 January 2017.

<sup>9</sup> Equifax, *About TrustedID Premier*, accessed at <https://www.equifaxsecurity2017.com/what-can-i-do/#about-trustedid-premier>, 23 October 2017.

expenses to clear ID theft problems up such as postage and notary fees. It doesn't usually reimburse you for money that's been stolen from you, and if it claims to cover attorney's fees, remember that such coverage is usually extremely limited.<sup>10</sup>

### III. Why there are Concerns with Credit Locks

There are several concerns with the more recently announced free lifetime lock on Equifax credit reports that is scheduled to be available as an app by the end of next January.<sup>11</sup> (The currently available lock is accessed by logging into an account via a web browser.)

From what we can tell, locks and freezes function similarly in that they block potential creditors like a bank or a lender from viewing your credit report.

The one difference we know of with Equifax's lock is that it does not block employment checks the way freezes do.<sup>12</sup> This difference does not raise concerns about fraud because ID thieves can't use employment checks to open accounts in your name. However, Experian's lock does not block access to employment checks or checks by insurance companies the way freezes do.<sup>13</sup> This could potentially leave consumers vulnerable to insurance fraud. TransUnion has not provided enough information to determine any functional differences.<sup>14</sup>

#### 1. There are Questions about Whether We'll Have to Give Up Our Rights with the Equifax Lock

Equifax's offer of its TrustedID Premier product after the breach came with strings attached – specifically signing away your rights to a day in court in the future. Signing up for the product required agreeing to "terms of use" that included an arbitration clause that potentially gave up your right to sue Equifax and join class action lawsuits over the breach.<sup>15</sup>

Due to public outcry, Equifax removed the arbitration language from its free TrustedID Premier product.

<sup>10</sup> Susan Grant, Director of Consumer Protection and Privacy, Consumer Federation, personal communication, 17 September 2015.

<sup>11</sup> While its website does not provide details about the new lifetime lock available next January, Richard Smith, the former CEO of Equifax said during Congressional hearings that it would be available as an app. See House Financial Services Committee, "Hearing entitled, 'Examining the Equifax Data Breach,'" 5 October 2017.

<sup>12</sup> Equifax, *About TrustedID Premier*, accessed at <https://www.equifaxsecurity2017.com/what-can-i-do/#about-trustedid-premier>, 23 October 2017.

<sup>13</sup> Experian's webpage about its lock product, Experian CreditLock, outlines who your credit report is and isn't accessible to when it is locked. It says that when locked, Experian credit reports are still accessible to, "potential employers or insurance companies during the application process." See Experian, *Experian CreditLock*, accessed at <https://www.experian.com/consumer-products/creditlock.html>, 23 October 2017.

<sup>14</sup> TransUnion's webpages about its lock service do not appear to include details about who it does and doesn't block access to. See TransUnion, *Credit Lock Plus – Equifax and TransUnion*, accessed at <https://www.transunion.com/product/credit-lock>, 23 October 2017 and TransUnion, *TrueIdentity Free Identity Protection*, accessed at <https://www.transunion.com/product/trueidentity-free-identity-protection>, 23 October 2017.

<sup>15</sup> Ron Lieber, "How to Protect Yourself After the Equifax Breach," *The New York Times*, updated 16 October 2017.

However, it still has an arbitration clause for other products on their website.

It's also unclear whether signing up for the free lifetime lock with Equifax available at the end of next January will require consumers to sign an agreement with an arbitration clause.<sup>16</sup>

## 2. We Already Have to Give Up Our Rights with the TransUnion and Experian Locks

TransUnion, which currently offers an unlimited free lock as part of its TruIdentity product does require signing an agreement with an arbitration clause.<sup>17</sup>

Experian does not offer a free lock and, according to the New York Times, has no interest in offering one.<sup>18</sup> But it does offer it as part of its paid credit monitoring services. Signing up for these services does require signing an arbitration agreement.<sup>19</sup>

## 3. There are Also Concerns about Privacy and Access with Making the Lock Available as an App

An app could collect data on users and send it back to Equifax and/or its vendors. Further, no one knows what "terms and conditions" or "privacy policy" will apply to users of the Equifax app. What additional information will the firm collect and what limits will be placed on its use? Will the terms be changeable at any time?

Apps require users to have smartphones with internet access. Freezes can be placed and lifted on web browsers and over the phone. It is unclear if Equifax's lifetime free lock will also be available on web browsers and over the phone.<sup>20</sup> TransUnion does not allow for locks to be placed over the phone.<sup>21</sup>

## 4. A Lock with One Bureau but Not the Others Leaves Consumers Vulnerable to Identity Theft

Aside from the numerous concerns above, getting a lock with Equifax but not the other two big bureaus is like locking your front door but leaving your garage and back doors wide open. Equifax is being negligent by not even telling consumers that they need to block access to their credit reports with all three bureaus.

<sup>16</sup> Ibid.

<sup>17</sup> TruIdentity, *Legal Information*, accessed at

<https://membership.trueidentity.com/tucm/support.page?panel=terms>, 23 October 2017.

<sup>18</sup> Ron Lieber, "Equifax Calls for Free Credit Locks. Experian's Reply? Nope," *The New York Times*, 4 October 2017.

<sup>19</sup> Experian, *Terms & Conditions*, accessed at [https://usa.experian.com/#/registration?offer=at\\_eiwpt102&br=exp](https://usa.experian.com/#/registration?offer=at_eiwpt102&br=exp), 23 October 2017.

<sup>20</sup> A brief description of the free lifetime lock on Equifax's General FAQs webpage says that, "...consumers will be able to use their smartphone or computer to lock and unlock their Equifax credit file directly and quickly." However, during a Congressional hearing, Equifax's former CEO, Richard Smith, said the difference with the lifetime lock over the current lock is that it will be an app on an iPhone. See Equifax, *FAQs*, accessed at <https://www.equifaxsecurity2017.com/frequently-asked-questions/>, 23 October 2017 and House Energy & Commerce Committee, "Oversight of the Equifax Data Breach," 3 October 2017.

<sup>21</sup> TransUnion's webpage about its free lock does not include information for getting a lock by phone. When I called TransUnion on October 19<sup>th</sup>, a representative told me that it was not possible to get a lock by the phone. See TransUnion, *TrueIdentity Free Identity Protection*, accessed at <https://www.transunion.com/product/trueidentity-free-identity-protection>, 23 October 2017.

The bottom line is that the best way to block access to credit reports is with freezes because they are a consumer right by law and not conditional on terms set by the credit bureaus.

#### IV. What We Need in Credit Freeze Legislation

Consumers should have the right, by law, to control access to our credit reports and protect ourselves from new account ID theft for free.

Equifax and the other credit bureaus fought for years against our right to freeze our credit reports in the first place and then demanded fees to do so.<sup>22</sup>

In fact, PIRG worked on the first security freeze law in California and then promoted it nationwide, state by state. We wrote a model data breach notice and security freeze law with Consumers Union/Consumer Reports and promoted it with many state AARP chapters.<sup>23</sup> Between 2005 and 2009 a version was passed by nearly every state, forcing the credit bureaus to eventually provide the freeze everywhere.

All 50 states and DC now have their own laws that determine the maximum amount that the credit bureaus can charge for credit freezes, temporary lifts or “thaws,” and permanent removals.<sup>24</sup>

Residents in only four states (Indiana, Maine, North Carolina and South Carolina) have access to free credit freezes and free thaws/temporary lifts. Residents in four other states (Colorado, Maryland, New Jersey and New York) have free freezes but charge for thaws. Three states (Delaware, Tennessee, Virginia) charge for freezes but provide free thaws.<sup>25</sup>

Approximately 158 million consumers between 18-65 in 42 states and DC must pay a fee to get credit freezes. If all consumers in those states between 18-65 choose to freeze their reports, that would cost them an estimated \$4.1 billion, under current laws.<sup>26</sup> (Even if you account for Equifax’s temporary waiving of fees to freeze Equifax reports until the end of next January, it would still cost consumer over \$2 billion dollars.)

We are not customers of the credit bureaus. We did not give them permission to collect and sell our info, and in the case of Equifax, to lose it. And now we have to pay to protect ourselves? We have to pay to control access to our own information?

<sup>22</sup> Here is an example of opposition to freeze legislation by the credit bureaus. Page 9 shows opposition to the first credit freeze law. See California Senate Judiciary Committee, *Bill Analysis SB 168*, accessed at <https://leginfo.ca.gov/faces/billAnalysisClient.xhtml>, 23 October 2017.

<sup>23</sup> U.S. Public Interest Research Group and Consumers Union, *The Clean Credit and Identity Theft Protection Act: Model State Laws*, November 2005.

<sup>24</sup> U.S. PIRG, *Credit Freezes By State*, accessed at <http://bit.ly/pirgfreezemap>, 23 October 2017.

<sup>25</sup> Only identity theft victims get freezes and thaws/lifts for free in every state. Some fees are waived, reduced, or even increased by some bureaus in some states for certain categories of consumers, including active duty servicemembers, victims of domestic violence, and minors. Ibid.

<sup>26</sup> Ibid.

The best way to protect consumers would be to freeze everyone's credit reports by default.<sup>27</sup> But making them free to all who take the step to opt in to get freezes would be a big win for consumers and an important first step with real benefits consumers deserve right now.

## **V. Federal Legislation Should Set a Floor, not a Ceiling for Security and Privacy Protections.**

We support federal legislation that sets free freezes for all Americans as the floor. We also support legislation that requires freezes to be placed within 15 minutes of an online or phone request, as is already the law in at least 10 states and DC.<sup>28</sup>

States should be allowed to continue finding even better ways to give consumers control over their credit reports. For example, a bill has been introduced in Massachusetts that not only makes the freeze free but also sets the freeze as the default on reports at all three credit bureaus.<sup>29</sup>

My testimony has focused on the need for free freeze legislation. But it's important that any federal legislation on other important issues about security and data also set the floor and not the ceiling on what states can do to better protect consumers.

For example, seven states and DC currently have data breach notification laws that require breach notification regardless of a risk assessment.<sup>30</sup> Twenty-six other states require notification of breaches that pose potential harms beyond narrow financial risks.<sup>31</sup> Several states, such as Massachusetts, also have comprehensive data security requirements. In past Congresses, bills that offer narrow breach notification and data security requirements have broadly preempted any broader state actions on privacy, breach notification, or data security.

Federal legislation should not preempt or replace existing stronger state laws.

## **VI: The Equifax Breach Serves Notice of the Need for Further Credit Reporting Reforms**

As discussed in much more detail today by Chi Chi Wu of the National Consumer Law Center, we also strongly support HR3755, the Comprehensive Consumer Credit Reporting Reform Act proposed by ranking member Maxine Waters and other members.<sup>32</sup> PIRG has worked with the committee since 1989

<sup>27</sup> Because credit freezes are the only way to prevent new account ID theft, the best public policy is for everyone's credit reports to be automatically frozen until consumers give consent to lift the freezes on their reports for credit checks.

<sup>28</sup> Transunion, *State Bill of Rights*, accessed at <https://www.transunion.com/docs/rev/personal/StateBillOfRights.pdf>, 23 October 2017.

<sup>29</sup> Attorney General Maura Healy, "Following Equifax Hack, AG Healey and Legislators Announce Data Breach Bill to Better Protect Massachusetts Residents", 25 September 2017.

<sup>30</sup> See Testimony of Laura Moy before the House Financial Services Committee regarding Financial Data Security in the Age of Computer Hackers, 14 May 2015, available at <https://financialservices.house.gov/calendar/eventsingle.aspx?EventID=399020>.

<sup>31</sup> Ibid.

<sup>32</sup> H.R. 3755 - *Comprehensive Consumer Credit Reporting Reform Act of 2017*, accessed at <https://www.congress.gov/bills/115th-congress/house-bill/3755%20U.S>, 23 October 2017.

in its oversight of the Big 3 credit bureaus or “consumer reporting agencies” (CRAs) and the Fair Credit Reporting Act (FCRA). While the transfer of FCRA responsibilities to the Consumer Bureau in 2011 has jump-started the Big 3’s compliance efforts, as Ms. Wu notes, HR3755 will make additional improvements to the law necessary to hold the CRAs accountable to consumers.

We also strongly oppose two bills that were the subject of a committee hearing on the date that the Equifax breach was disclosed to consumers.<sup>33</sup> HR2359 (Rep. Loudermilk), the “FCRA Liability Harmonization Act” would wrongly eliminate all punitive damages and cap other damages when consumer reporting agencies break the law, eliminating a strong incentive to comply with the law. A discussion draft from Rep. Royce of the committee known as the “Facilitating Access to Credit Act,” would exempt consumer reporting agency (and certain other firms’) credit monitoring and other “educational” products from the Credit Repair Organizations Act, replacing strong protections against deceptive promises with a weak regulatory scheme.

## Conclusion

One of the data breaches featured in our freeze report two years ago was where Experian, a different credit bureau, lost data including social security numbers and birthdates for 15 million T-Mobile customers.<sup>34</sup>

The national discourse didn’t change after that breach, and necessary laws were not passed. But the national discourse is changing this time and hopefully will be accompanied by action.

The only kind of ID theft that can be stopped before it happens once personal information has been stolen is new account ID theft. And the only way to prevent that is by blocking access to your credit reports at all three big national credit bureaus. It’s time for consumers to have the right by law to protect themselves and control access to their own reports with credit freezes for free.

Thank you for your attention on this important issue and for the opportunity to present my testimony.

<sup>33</sup> House Financial Services Committee, “Hearing entitled, ‘Legislative Proposals for a More Efficient Federal Financial Regulatory Regime,’” 7 September 2017.

<sup>34</sup> Ed Mierzwinski and Mike Litt, U.S. PIRG, *Why You Should Get Credit Freezes Before Your Information is Stolen*, October 2015.



STATE OF NEW YORK  
OFFICE OF THE ATTORNEY GENERAL

ERIC T. SCHNEIDERMAN  
ATTORNEY GENERAL

DIVISION OF ECONOMIC JUSTICE  
BUREAU OF INTERNET & TECHNOLOGY

**PREPARED STATEMENT OF KATHLEEN MCGEE  
CHIEF OF THE BUREAU OF INTERNET & TECHNOLOGY  
NEW YORK STATE OFFICE OF THE ATTORNEY GENERAL  
TO THE HOUSE FINANCIAL SERVICES COMMITTEE**

**OCTOBER 25, 2017**

Mr. Chairman, Madam Ranking Member, and other distinguished Members of the Committee:

My name is Kathleen McGee, and I am the Chief of the Bureau of Internet & Technology at the New York State Office of the Attorney General, Eric T. Schneiderman. The Bureau of Internet & Technology is responsible for protecting New Yorkers from existing as well as new and developing online threats.

I am pleased to present this prepared testimony concerning data breaches, which continue to victimize consumers with greater and greater frequency, from small local businesses to giants like Target, Anthem, Yahoo, and now Equifax.

The Equifax data breach was unprecedented in scale and severity, affecting the private information of 145 million Americans, including more than 8 million New Yorkers. Our office acted immediately, launching a formal investigation of Equifax and pressing the company on a number of issues – including a delay in notifying consumers of the breach, a forced arbitration clause in free credit monitoring contracts, and the failure to provide Spanish-language customer service to consumers affected by the breach. Following conversations with our office, Equifax addressed all of those issues and later agreed to provide consumers the ability to lock and unlock their credit file for life.

We also contacted the other major credit bureaus – TransUnion and Experian – to discuss their data security.

We have also been in touch with numerous other state AG's offices – since we states often lead in consumer protection and data breach matters – as well as various federal agencies. While I cannot share details from ongoing investigations, I can say we are getting to the bottom of the Equifax breach and will ensure that all credit bureaus take effective steps to protect the sensitive information that millions of Americans have entrusted to them.

States have a central role in protecting consumers and their data. The New York Attorney General's Office and other state Attorneys General offices have been policing data breaches for nearly two decades.

Indeed, the states led the way on data protection for consumers. When the internet was still relatively new to consumers, states responded with data protection and data breach laws to protect their residents. And as the technology has evolved over the years, state law has evolved with it.

Back in 2002, when the internet was younger and e-commerce was beginning to take off, the state of California enacted the first data breach notification law. It proved to be a tremendous success for consumer protection, and New York and other states soon followed. Today, 48 states plus DC and the U.S. territories all have data breach notification laws. That is the sort of innovation at the state level that our federal system, at its best, promotes.

The states have already adapted those laws as technology and consumers' use of it changed, and as new threats emerged. For example, as email and other online accounts became an increasing part of consumers' daily lives – to make appointments, send confidential documents, and discuss work and personal affairs – account credentials became the “keys to the castle” for consumers' data.

As a result, states amended their laws to add username-and-password combinations as a trigger for breach notification – a key state law innovation. This is just one of many examples. As healthcare records increasingly became digitized, state laws began covering patient data. As companies increasingly used fingerprints to unlock devices, state laws began covering biometric data.

But it is better to prevent breaches before they happen. And states have been equally innovative on this point: enacting legislation requiring companies to implement adequate data security, and updating such laws as technology evolves. And states have a second tool: consumer protection laws, which AGs use to police misrepresentations about data security – as with other consumer products, it can be unlawful for a company to make misrepresentations about data security to consumers.

The New York Attorney General's office, recognizing the importance of this issue for consumers and the need to update New York's law, has proposed legislation to update New York's data security and breach notification laws. And, the New York Department of Financial Services – a separate state agency with jurisdiction over New York's banking and insurance sectors – also has innovated in this area, implementing important data security regulations to protect consumers' financial data.

In light of this background, I would like to make a few key points.

First, it would be a big mistake for Congress to preempt states' ability to legislate and innovate in this area. The law must be able to keep pace with the ever-increasing rate of change



in technology. States have proven the ability to act quickly in that regard – from both legislative and enforcement perspectives. In contrast, bills have been proposed in Congress for many years but, for one reason or another, enactment has proven elusive. Even if a federal law were enacted, it could prove difficult to amend and would fall far behind new technologies that will inevitably continue to emerge. Thus, even a federal law providing the most stringent protections based on current state requirements will leave consumers more and more vulnerable over time.

Second, when it comes to enforcement, states occupy a leading role today and must continue to do so.

Our office has issued data breach reports in recent years that show an alarming increase in data breaches. Indeed, in 2016 we received 1,300 data breach notices – up 60% from the year before. This Committee is likely aware of the megabreaches, such as the Target breach involving 40 million credit card numbers and the Anthem breach involving over 78 million records including Social Security Numbers. In those instances, New York and other states used a well-established process to coordinate enforcement efforts against companies that violated consumer trust with inadequate data security. As a result, the states obtained not just data security reforms through injunctive relief, but also large civil penalty recoveries that are essential to deterring other companies from violating consumer trust through lax security practices.

Less well-known, yet equally important, are the enforcement actions our office takes in response to smaller breaches that occur by the hundreds each year in New York and other states. One recent case illustrates the point. A small company outside Buffalo, New York misconfigured a web server, which led to the disclosure of 500 employment applications with Social Security Numbers in Google search results. Our office found out through a tip, contacted the company immediately, and got the applications removed from search results within days.

Even if a federal agency were provided with the most comprehensive data security law and the considerable resources needed for serious enforcement, it is unlikely that a federal agency would be as responsive as our office and our sister state AG's offices to breaches involving local businesses and relatively small numbers of local consumers. These breaches may be smaller than a Target or an Equifax – but the victims are no less in need of law enforcement protection. Smaller breaches like these are the rule, not the exception.

Further, with years of first-hand experience policing data security in our state, we know how to distinguish between breaches that a company should have prevented with better security versus breaches that could not have been avoided despite the company's reasonable security practices. By virtue of this experience, and our knowledge of conditions within our local communities and industries, we can avoid both underenforcement that would leave consumers unduly vulnerable and overenforcement that would create undue burdens on local businesses.

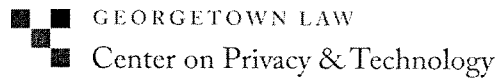
For all of these reasons, I respectfully urge this Committee to ensure that any legislation it considers meets the following requirements, which are vital to protecting states' innovative role in consumer data protection:

- Any new federal requirements should not preempt state law, but instead should expressly set a floor—not a ceiling—on data security standards and protocols in the event of breaches. States must be able to innovate in the areas of data security and breach notification and pass stronger and more up-to-date laws than the federal standard.
- As with several other federal consumer protection laws, any federal requirements must be enforceable by state attorneys general in addition to a federal agency, and any federal penalties or other monetary relief must be recoverable by the states as well.
- To the extent any preemption language is included, beyond the floor/ceiling issue discussed above, the language must be drawn carefully to avoid unintended severe consequences. Some preemption language can be so broad that it might be interpreted to set aside state laws concerning personal privacy or computer crimes, and that would be a serious problem for constituents.

These or similar provisions for joint federal and state enforcement authority are already included in other federal laws and have proven successful. For example, the New York AG's office has coordinated with the FTC on several investigations into violations of the federal Children's Online Privacy Protection Act, or COPPA, to stop invasive tracking on major child-focused websites.

The vast majority of state AGs' offices have similarly called on Congress to avoid preempting state action on data security, as recently as 2015, when a broad bipartisan group of 45 state AGs joined in asking Congress to oppose then-pending data security bills with harmful preemption provisions.

Our office continues to enforce data security protections on behalf of New Yorkers and to work with New York's state lawmakers to continually update those protections. We appreciate your Committee's efforts to complement those efforts at the federal level while ensuring that work at the state will continue successfully.



**Statement of Laura Moy, Deputy Director  
Center on Privacy & Technology at Georgetown Law**

*Before the*

**U.S. House of Representatives  
Financial Services Committee**

*Hearing on*

**Continuation of Hearing Entitled  
"Examining the Equifax Data Breach"**

Wednesday, October 25, 2017

For more information, contact Laura Moy at [laura.moy@georgetown.edu](mailto:laura.moy@georgetown.edu).

### Introduction and Summary

Chairman Hensarling, Ranking Member Waters, and Members of the Committee:

Thank you for working to study and address data security and data breaches, and for the opportunity to testify on this important issue. I am the Deputy Director of the Center on Privacy & Technology at Georgetown University Law Center,<sup>1</sup> a think tank focused on privacy and surveillance law and policy. Today I represent my individual views on the Equifax data breach, data security, and breach notification, and not the views of my employer.

Consumers deserve better than this. They have no choice but to share highly private information with financial institutions in order to participate in the modern economy, and simply must trust that those institutions will do their absolutely best to safeguard that information. Equifax failed Americans, and nearly half of us—myself included—are going to be paying for that failure with a heightened risk of identity theft for the rest of our lives.

That is why hearings like this one, to interrogate the state of data security in our country today and to discuss ways that we might improve upon the status quo, are so important. As we try to move forward from the Equifax breach, I offer this Committee a few recommendations:

- Enhance the authority of federal agencies to oversee the data security practices of consumer reporting agencies, to promulgate rules governing the data security obligations of financial institutions, and to enforce those obligations with civil penalties
- Streamline the credit freeze process
- Establish protective tools for victims of child identity theft and medical identity theft

---

<sup>1</sup> I am very grateful for the assistance of four law student research assistants who assisted in the preparation of this testimony: Caroline Zitin, Eric Olson, Pia Benosa, and Zach Noble.

- Prohibit mandatory arbitration clauses designed to keep victims of data security or privacy violations out of court
- Avoid advancing legislation that weakens or eliminates consumer protections that currently exist at the state level
- Ensure that any federal legislation designed to enhance data security and/or breach notification standards includes regulatory flexibility to adapt to shifting threats
- Ensure that any federal legislation designed to enhance data security and/or breach notification standards includes enforcement authority for state attorneys general

I thank you for this opportunity and I look forward to answering your questions.

#### 1. **Equifax Made Mistakes**

There is no question that Equifax made serious mistakes. Equifax could and should have prevented a breach of this magnitude from occurring. Indeed, the scale of the breach alone—affecting some 45% of American consumers in an attack that took place over the course of months—indicates that Equifax’s security program was riddled with problems. And it was. Equifax’s unreasonable security failures include the failure to encrypt the large volume of data that ultimately was exfiltrated by attackers,<sup>2</sup> the months-long failure to patch the critical Apache Struts vulnerability that was

---

<sup>2</sup> *Oversight of the Equifax Data Breach: Answers for Consumers: Hearing Before the H. Comm. on Energy and Commerce Subcomm. on Digital Commerce and Consumer Protection*, 115th Cong. (Oct. 3, 2017) (statement of Richard F. Smith, Former Chairman and CEO, Equifax, Inc.), preliminary transcript at 81, *available at* <http://docs.house.gov/meetings/IF/IF17/20171003/106455/HHRG-115-IF17-Transcript-20171003.pdf> (“To be very specific this data was not encrypted at rest.”) [hereinafter *Oct. 3 Hearing*]

exploited,<sup>3</sup> the apparent lack of appropriate management and redundancies to ensure the patch would be applied,<sup>4</sup> and the months-long failure to detect the breach even as attackers continued to access and steal sensitive consumer data. These failures are well documented elsewhere,<sup>5</sup> so I will not elaborate on them.

Making matters worse, Equifax bungled post-breach activities as well.<sup>6</sup> First, Equifax did not directly notify affected consumers.<sup>7</sup> Instead, Equifax required consumers to visit a website to check whether they had been affected by the breach, but constructed that website on an unfamiliar domain (i.e. not Equifax.com) newly registered for that express purpose, which created confusion and introduced phishing vulnerabilities.<sup>8</sup> Second, Equifax's

---

<sup>3</sup> See Lily Hay Newman, *Equifax Officially Has No Excuse*, WIRED (Sept. 14, 2017), <https://www.wired.com/story/equifax-breach-no-excuse/>.

<sup>4</sup> *Oct. 3 Hearing* (statement of Richard F. Smith, Former Chairman and CEO, Equifax, Inc.), preliminary transcript at 35, ("The human error was the individual who is responsible for communicating in the organization to apply the patch did not."); see Russell Brandom, *Former Equifax CEO Blames Breach on a Single Person Who Failed to Deploy Patch*, The Verge (Oct. 3, 2017), <https://www.theverge.com/2017/10/3/16410806/equifax-ceo-blame-breach-patch-congress-testimony>.

<sup>5</sup> See, e.g., Complaint, Commonwealth of Massachusetts v. Equifax, Inc. (Sept. 19, 2017), available at <http://www.mass.gov/ago/docs/press/2017/equifax-complaint.pdf>.

<sup>6</sup> See Brian Krebs, *Equifax Breach Response Turns Dumpster Fire*, Krebs on Security (Sept. 8, 2017), <https://krebsonsecurity.com/2017/09/equifax-breach-response-turns-dumpster-fire/>.

<sup>7</sup> *Examining the Equifax Data Breach: Hearing Before the H. Comm. on Financial Services*, 115th Cong. (Oct. 5, 2017) (dialogue between Rep. Brad Sherman and Richard F. Smith, Former Chairman and CEO, Equifax, Inc.), transcript not yet available (Rep. Sherman: "Is it the intention of Equifax to send a notice to those whose . . . data were compromised? Or is it up to them to go to your difficult-to-use, overburdened website to find out?" Smith: "We followed what we thought was due process. We sent out press releases, set up . . . a website, a phone number." Sherman: "How about noticing? Are you going to give notice to the 143 million people? Are you going to send them a letter?" Smith: "No, sir.").

<sup>8</sup> Dani Deahl & Ashley Carman, *For Weeks, Equifax Customer Service Has Been Directing Victims to a Fake Phishing Site*, The Verge (Sept. 20, 2017), <https://www.theverge.com/2017/9/20/16339612/equifax-tweet-wrong-website->

call center and website were overwhelmed by visits from concerned consumers, many of whom found themselves completely unable to get through.<sup>9</sup> On top of all that, some Equifax executives are facing allegations of insider trading related to the breach.<sup>10</sup>

Consumers are justifiably outraged. The 165.5 million Americans whose private details were breached in the Equifax attack now face an increased risk of identity theft in perpetuity. Now that their names, Social Security numbers, and other difficult-to-change data closely tied to financial records have been breached, those details are out there forever—there is no putting the genie bac in the bottle.

Equifax's failures are all the more infuriating because consumers are not given a choice about whether or not their information will be shared with consumer reporting agencies (CRAs) like Equifax. The massive troves of valuable and potentially damaging information that CRAs maintain are provided by furnishers, not by consumers themselves.

And the consumers who suffer the worst are those who lack the time, resources, or technical sophistication to research and secure credit freezes or credit monitoring services. Even individuals with relatively sophisticated understanding of credit and the CRAs have expressed frustration with these

phishing-identity-monitoring ("Full-stack developer Nick Sweeting set up the misspelled phishing site in order to expose vulnerabilities that existed in Equifax's response page. 'I made the site because Equifax made a huge mistake by using a domain that doesn't have any trust attached to it [as opposed to hosting it on equifax.com],' Sweeting tells *The Verge*. 'It makes it ridiculously easy for scammers to come in and build clones — they can buy up dozens of domains, and typo-squat to get people to type in their info.'").

<sup>9</sup> Michelle Singletary, *Equifax Says It's Overwhelmed. Its Customers Say They Are Getting the Runaround*, Wash. Post (Sept. 19, 2017), <https://www.washingtonpost.com/news/get-there/wp/2017/09/19/equifax-says-its-overwhelmed-its-customers-say-they-are-getting-the-runaround/>.

<sup>10</sup> Tom Schoenberg, Anders Melin, & Matt Robinson, *Equifax Stock Sales Are the Focus of U.S. Criminal Probe*, Bloomberg (Sept. 18, 2017), <https://www.bloomberg.com/news/articles/2017-09-18/equifax-stock-sales-said-to-be-focus-of-u-s-criminal-probe>.

tools, which may therefore be unavailable as a practical matter to many under-resourced consumers.

**2. Federal Legislation Should Set a Strong Consumer Protection Standard to Address Problems Highlighted by the Equifax Breach**

Consumers need more control over their personal data, and companies need stronger incentives to improve data security. Congress should advance federal legislation to subject CRAs to closer regulatory oversight and stronger enforcement, and to enhance consumers' control of their own personal information.

**A. Congress Should Consider Subjecting the Security Practices of Consumer Reporting Agencies to Closer Regulatory Oversight and Stronger Enforcement**

First and foremost, Congress should consider vesting a federal agency or agencies with the authority to more closely regulate and enforce the data security practices of CRAs. Members of this committee and others have expressly called for the Federal Trade Commission (FTC) and the Consumer Financial Protection Bureau (CFPB) to examine the Equifax breach and take enforcement action in response to poor security practices. Both agencies appear to be looking into the Equifax breach. But to help prevent similar breaches from occurring in the future, Congress should explore bolstering these agencies' authority to promulgate rules governing the data security practices of CRAs, to conduct ongoing review of CRAs' data security practices, to enforce rules, and to seek civil penalties for violations.

At this point, the FTC has rulemaking and enforcement authority over CRAs' data security practices, but no supervisory authority. In accordance with the Gramm-Leach-Bliley Act (GLBA), in 2002 the FTC promulgated the Safeguards Rule,<sup>11</sup> which governs the data security obligations of financial

---

<sup>11</sup> 16 C.F.R. §314



institutions, including CRAs.<sup>12</sup> Companies covered by the rule not only must align their own data security practices with the requirements of the rule, but also must ensure that their affiliates and service providers safeguard customer information in their care.<sup>13</sup> But as the Congressional Research Service explains, the FTC “has little up-front supervisory or enforcement authority, making it difficult to prevent an incident from occurring and instead often relying on enforcement after the fact.”<sup>14</sup>

The CFPB, on the other hand, has exercised supervisory authority over CRAs since 2012, but lacks the authority to promulgate rules implementing or to enforce the data security provisions of GLBA.<sup>15</sup> Title X of the Dodd-Frank Act granted the CFPB rulemaking authority for much of GLBA, but according to the CFPB itself, Dodd-Frank “excluded financial institutions’ information security safeguards under GLBA Section 501(b) from the CFPB’s rulemaking, examination, and enforcement authority.”<sup>16</sup>

In addition, Congress should consider urging the FTC and/or CFPB to complete a notice and comment rulemaking process to update the Safeguards Rule. The existing Safeguards Rule was promulgated in 2002. In 2016 the FTC began the process of updating that rule, and solicited public comment on a number of both questions, including about the substantive standards set forth in the rule, such as, “Should the Rule be modified to include more specific and prescriptive requirements for information security plans?” and “Should the Rule be modified to reference or incorporate any other

---

<sup>12</sup> Fed. Trade Comm’n, *Financial Institutions and Customer Information: Complying with the Safeguards Rule*, <https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying> (last visited Oct. 23, 2017).

<sup>13</sup> *Id.*

<sup>14</sup> N. Eric Weiss, *The Equifax Data Breach: An Overview and Issues for Congress*, CRS Insight (Sept. 29, 2017) at 2.

<sup>15</sup> *Id.*

<sup>16</sup> Consumer Fin. Protection Bureau, *Privacy of Consumer Financial Information – Gramm-Leach-Bliley Act (GLBA) Examination Procedures* at 1 (Oct. 2016), [https://s3.amazonaws.com/files.consumerfinance.gov/f/documents/102016\\_cfpb\\_GLBAExamManualUpdate.pdf](https://s3.amazonaws.com/files.consumerfinance.gov/f/documents/102016_cfpb_GLBAExamManualUpdate.pdf).

information security standards or frameworks, such as the National Institute of Standards and Technology's Cybersecurity Framework or the Payment Card Industry Data Security Standards?"<sup>17</sup> The FTC has not completed the update. Most recently, in June, the FTC published a notice indicating that the Safeguards Rule is "currently under review," and that the agency does not expect to complete the review in 2017.<sup>18</sup>

Congress should also consider giving one or both agencies the authority to seek civil penalties for violations of the Safeguards Rule. The FTC has itself called for civil penalty authority in the past to buttress its data security authority. As now-Acting Chairman of the FTC (then a Commissioner) Maureen Ohlhausen argued in remarks she delivered before Congressional Bipartisan Privacy Caucus in 2014,

Legislation in both areas – data security and breach notification – should give the FTC the ability to seek civil penalties to help deter unlawful conduct, rulemaking authority under the Administrative Procedure Act, and jurisdiction over non-profits. Under current laws, the FTC only has the authority to seek civil penalties for data security violations with regard to children's online information under COPPA or credit report information under the FCRA.<sup>19</sup> To help ensure effective deterrence, we urge Congress to allow the FTC to seek civil penalties for data security and breach notice violations in appropriate circumstances.<sup>20</sup>

---

<sup>17</sup> FTC Standards for Safeguarding Customer Information, Request for Public Comment, 81 Fed. Reg. 173 (Sept. 7, 2016), [https://www.ftc.gov/system/files/documents/federal\\_register\\_notices/2016/09/frn\\_standards\\_for\\_safeguarding\\_customer\\_information.pdf](https://www.ftc.gov/system/files/documents/federal_register_notices/2016/09/frn_standards_for_safeguarding_customer_information.pdf).

<sup>18</sup> FTC Regulatory Review Schedule, 82 Fed. Reg. 123 (June 28, 2017), [https://www.ftc.gov/system/files/documents/federal\\_register\\_notices/2017/06/reg\\_review\\_schedule\\_published\\_frns.pdf](https://www.ftc.gov/system/files/documents/federal_register_notices/2017/06/reg_review_schedule_published_frns.pdf).

<sup>19</sup> The FTC can also seek civil penalties for violations of administrative orders. 15 U.S.C. § 45(j) (footnote in original).

<sup>20</sup> Maureen Ohlhausen, Commissioner, Fed. Trade Comm'n, Remarks Before the Congressional Bipartisan Privacy Caucus (Feb. 3, 2014), transcript

To improve the FTC's and CFPB's ability to protect Americans from poor data security practices of financial institutions that house extremely sensitive information, Congress should consider vesting one or both agencies with full-throated supervisory, rulemaking, and enforcement authority, and consider urging the update of the Safeguards Rule.

**B. Congress Should Consider Expanding Consumer Tools for Redress in the Event of a Breach**

In addition to taking steps to bolster regulatory and enforcement authority to help prevent similar breaches from taking place in the future, Congress should consider giving consumers better tools for redress when their personal information is compromised in a future breach. Specifically, Congress should consider streamlining the credit freeze process, establishing protective tools for victims of child identity theft and medical identity theft, and prohibiting mandatory arbitration clauses.

The credit freeze process is overdue for an overhaul—although credit freezes offer useful protection, they can be tedious, inconvenient, and costly. The credit freeze is, according to U.S. PIRG, “your best protection against someone opening new credit accounts in your name,”<sup>21</sup> and the IRS encourages consumers to consider requesting a freeze “if you were part of a large-scale data breach.”<sup>22</sup> But the FTC cautions consumers considering a credit freeze to “[c]onsider the cost and hassle factor,” because a credit freeze

---

available at [https://www.ftc.gov/system/files/documents/public\\_statements/remarks-commissioner-maureen-k.ohlhausen/140203datasecurityohlhausen.pdf](https://www.ftc.gov/system/files/documents/public_statements/remarks-commissioner-maureen-k.ohlhausen/140203datasecurityohlhausen.pdf).

<sup>21</sup> Mike Litt & Edmund Mierzwinski, U.S. PIRG, *Why You Should Get Credit Freezes Before Your Information Is Stolen: Tips to Protect Yourself Against Identity Theft & Financial Fraud* at 1 (Oct. 2015), available at [https://uspirg.org/sites/pirg/files/reports/USPIRGFREEZE\\_0.pdf](https://uspirg.org/sites/pirg/files/reports/USPIRGFREEZE_0.pdf).

<sup>22</sup> Internal Revenue Service, *Tips for Using Credit Bureaus to Help Protect Your Financial Accounts*, <https://www.irs.gov/newsroom/tips-for-using-credit-bureaus-to-help-protect-your-financial-accounts> (last visited Oct. 23, 2017).

can delay access to credit, is only truly effective if secured across all three major CRAs, and may come at a cost of \$5 to \$10 for each CRA every time a consumer wishes to freeze or thaw their credit.<sup>23</sup> Congress should consider requiring CRAs to make it faster, easier, and free for consumers to freeze or thaw their credit, and to work together to ensure that a credit freeze or thaw request made with one CRA is applied to other bureaus as well. A protective tool like the credit freeze should be simplified so that consumers can easily access it, and should not be made available only to those consumers who can afford to pay for it either in time or in dollars.

Congress should also consider expanding the suite of tools that the law requires be made available to help consumers who become victims of identity theft. For consumers of financial identity theft, there are modest protections in place, including enhanced free credit monitoring and fraud alert options. But for other forms of identity theft, such as child identity theft and medical identity theft, no such tools exist. Congress should consider providing these victims with the tools they'll need to protect their identity—and if stolen, restore it.

In addition, Congress should consider prohibiting the use of mandatory arbitration clauses designed to keep consumers who have been the victim of data security or privacy violations out of court. Equifax invited tremendous criticism for its inclusion of a forced arbitration clause in the terms made available to individuals subject to its breach, and has since stated that it never intended to include the arbitration clause.<sup>24</sup> Congress should make clear that mandatory arbitration is never permissible where the privacy and data security obligations of financial institutions are concerned.

---

<sup>23</sup> Lisa Weintraub Schifferle, Fed. Trade Comm'n, *Fraud Alert or Credit Freeze – Which Is Right for You?* (Sept. 14, 2017), <https://www.consumer.ftc.gov/blog/2017/09/fraud-alert-or-credit-freeze-which-right-you> (last visited Oct. 23, 2017).

<sup>24</sup>

**3. Congress Should Not Issue Federal Data Security or Breach Notification Legislation that Eliminates Existing Consumer Protections**

As I have argued before this committee in the past, many states are currently doing a very good job passing and adjusting data security and breach notification laws to respond to developing threats, monitoring threats to residents, guiding small businesses, and selectively bringing enforcement actions against violators. Therefore, if Congress considers passing federal legislation on data security and breach notification, consumers would best be served by a bill that does not preempt state laws. If Congress nevertheless considers legislation that does preempt state data security and breach notification provisions, I urge you to explore legislation that is narrow, and that merely sets a floor for disparate state laws—not a ceiling.

In the event, however, that Congress nevertheless seriously considers broad preemption, the new federal standard should strengthen, or at the very least preserve, important protections that consumers currently enjoy at the state level. In particular, federal legislation:

- 1) should not ignore the serious physical, emotional, and other non-financial harms that consumers could suffer as a result of misuses of their personal information,
- 2) should not eliminate data security and breach notification protections for types of data that are currently protected under state law,
- 3) should provide a means to expand the range of information protected by the law as technology develops,
- 4) should include enforcement authority for state attorneys general, and

- 5) should be crafted in such a way as to avoid preempting privacy and general consumer protection laws.<sup>25</sup>

**A. Federal Legislation Should Address Physical and Emotional Harms that Consumers Could Suffer as a Result of Misuses of Their Personal Information**

This Committee's attention to the issue of data security and breach notification is driven first and foremost by the threat of identity theft and related financial harms. Thus some legislation that this Committee has considered in the past would allow covered entities to avoid notifying customers of a breach if they determine that there is no risk of financial harm. Such "harm triggers" in breach notification bills are problematic, because it is often very difficult to trace a specific harm to a particular breach, and because after a breach has occurred, spending time and resources on the completion of a risk analysis can delay notification. Moreover, a breached entity may not have the necessary information—or the appropriate incentive—to effectively judge the risk of harm created by the breach.

In addition, trigger standards narrowly focused on financial harm ignore the many non-financial harms that can result from a data breach. For example, an individual could suffer harm to dignity if he stored embarrassing photos in the cloud and those photos were compromised. If an individual's personal email were compromised and private emails made public, she could suffer harm to her reputation. And in some circumstances, breach could even lead to physical harm. For example, the fact that a domestic violence victim had called a support hotline or attorney, if it fell into the wrong hands, could endanger her life.

---

<sup>25</sup> These points are closely related to concerns I have previously presented before this Committee. See Testimony of Laura Moy before the House of Representatives Financial Services Committee Hearing on Protecting Consumers: Financial Data Security in the Age of Computer Hackers, available at <https://financialservices.house.gov/UploadedFiles/HHRG-114-BA00-WState-LMoy-20150514.pdf>.

Many state laws recognize these various types of non-financial harms. Accordingly, many states and the District of Columbia either require breach notification regardless of a risk assessment, or, if they do include some kind of harm trigger, take into account other types of harms beyond the strictly financial. There is no harm trigger at all in a handful of states, including, notably, California<sup>26</sup> and Texas.<sup>27</sup> In a majority of states, although the duty to notify is conditioned on a trigger, the trigger is not explicitly limited to risk of financial harm, and arguably encompasses non-financial harms as well. States in this category include Alaska,<sup>28</sup> Delaware,<sup>29</sup> Maryland,<sup>30</sup> North Carolina,<sup>31</sup> and Pennsylvania.<sup>32</sup>

A bill with a narrow financial harm trigger that preempts state laws that contemplate other types of harm would thus constitute a step backwards for many consumers. To address this problem, any legislation the Committee considers should either limit preemption so as to leave room for states to require notification even in circumstances where the harm is not clear or is

---

<sup>26</sup> Cal. Civ. Code § 1798.29.

<sup>27</sup> Tex. Bus. & Com. Code § 521.053.

<sup>28</sup> Alaska Stat. § 45.48.010 (notification not required if “the covered person determines that there is not a reasonable likelihood that harm to the consumers whose personal information has been acquired has resulted or will result from the breach”).

<sup>29</sup> Del. Code tit. 6, § 12B-102 (notification not required if, “after an appropriate investigation, the person reasonably determines that the breach of security is unlikely to result in harm to the individuals whose personal information has been breached”).

<sup>30</sup> Md. Code Ann. Com. Law § 14-3504 (notification required if “the business determines that misuse of the individual’s personal information has occurred or is reasonably likely to occur as a result of a breach of the security of a system”).

<sup>31</sup> N.C. Gen. Stat. § 75-61 (definition of “security breach” limited to situations in which “illegal use of the personal information has occurred or is reasonably likely to occur or that creates a material risk of harm to a consumer”); *see* N.C. Gen. Stat. § 75-65.

<sup>32</sup> 73 Pa. Stat. Ann. § 2302 (definition of “breach of the security of the system” limited to situations in which unauthorized access “causes or the entity reasonably believes has caused or will cause loss or injury to any resident of this Commonwealth”).

not financial in nature, or include a trigger provision as inclusive as the most inclusive state-level triggers.

**B. Federal Legislation Should Not Eliminate Data Security and Breach Notification Protections for Types of Data Currently Protected Under State Law**

Many privacy and consumer advocates are concerned about recent legislative proposals on data security and breach notification that define the protected class of personal information too narrowly. A definition narrower than that of state data security and breach notification laws, in combination with broad preemption, would weaken existing protections in a number of states.

For example, under California law, entities must implement and maintain reasonable security procedures and practices to protect—and notify consumers of unauthorized access to—“[a] username or email address in combination with a password or security question and answer that would permit access to an online account.”<sup>33</sup> Not only does coverage for online account login credentials help protect accounts holding private, but arguably non-financial, information such as personal emails and photographs, but it often protects a range of other online accounts, because many consumers recycle the same password across multiple accounts. To illustrate, consider when, in 2015, Uber accounts were hacked into, resulting in fraudulent charges to customers for rides they never took. Reporter Joseph Cox wrote about how those accounts may have been broken into using login credentials for unrelated accounts that were disclosed in other breaches:

First, a hacker will get hold of any of the myriad data dumps of email and password combinations that are circulated in the digital underground. This list of login details will then be loaded into a computer program along with the Uber website

---

<sup>33</sup> Cal. Civ. Code §§ 1798.29; 1798.81.5.



configuration file. From here, the program will cycle through all of the login credentials and try them on the Uber website, in the hope that they have also been used to set up an Uber account.

“It’s basically checking a database dump/account list against a certain website and displaying results,” [a hacker who calls himself] Aaron told Motherboard over encrypted chat.

Aaron then demonstrated this process, and had accessed an Uber account within minutes. He tested 50 email and password combinations sourced from a leak of a gaming website, and two worked successfully on Uber. Aaron claimed one of these was a rider’s account, and he then sent several censored screenshots of the user’s trip history and some of their credit card details.<sup>34</sup>

A number of state laws also require private entities to protect information about physical and mental health, medical history, and insurance, including laws in California,<sup>35</sup> Florida,<sup>36</sup> and Texas.<sup>37</sup> This is important because attackers use information about health and medical care to facilitate medical identity theft, a rapidly growing threat.<sup>38</sup> Not only does medical identity theft often result in enormous charges to a patient for medical care she never received, but it can also pollute her medical record with false information about her health status, which could lead to additional

---

<sup>34</sup> Joseph Cox, *How Hackers Can Crack People’s Uber Accounts to Sell on the Dark Web*, Medium (May 4, 2015), <http://motherboard.vice.com/read/how-hackers-cracked-peoples-uber-accounts-to-sell-on-the-dark-web>.

<sup>35</sup> Cal. Civ. Code § 1798.81.5.

<sup>36</sup> Fla. Stat. § 501.171.

<sup>37</sup> Tex. Bus. & Com. Code § 521.002.

<sup>38</sup> Ponemon Institute, *Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data* (2016), available at <https://www.ponemon.org/local/upload/file/Sixth%20Annual%20Patient%20Privacy%20%26%20Data%20Security%20Report%20FINAL%206.pdf>; Michelle Andrews, *The Rise of Medical Identity Theft*, Consumer Reports (Aug. 25, 2016), <https://www.consumerreports.org/medical-identity-theft/medical-identity-theft/>.

complications or even physical harm down the road.<sup>39</sup> Health and medical information can also be used to inform spear phishing attacks, in which an attacker posing as a medical or insurance provider sends a fake bill or email to a patient asking for billing information related to recent treatment, thus tricking the patient into providing sensitive financial information.

North Dakota's breach notification law protects electronic signature, date of birth, and mother's maiden name, all pieces of information that could be used to verify identity for the purpose of fraudulently creating or logging into an online or financial account.<sup>40</sup>

Some states are also now requiring entities to take steps to protect biometric data.<sup>41</sup> This important step recognizes that a biometric identifier such as a fingerprint or iris scan cannot be changed by the individual to whom it belongs. Some states that now require protection of biometric data include Connecticut<sup>42</sup> and New Mexico.<sup>43</sup>

Health and medical information, login credentials for online accounts, and electronic signatures are just a few important categories of private information that would not be covered by a number of federal legislative proposals that have been under consideration in past years. At the same time, many of those same proposals would have preempted all of the above-referenced state laws that *do* protect that information, substantially

---

<sup>39</sup> See Joshua Cohen, *Medical Identity Theft—The Crime that Can Kill You*, MLMIC Dateline (Spring 2015), available at [https://www.mlmic.com/wp-content/uploads/2014/04/Dateline-SE\\_Spring15.pdf](https://www.mlmic.com/wp-content/uploads/2014/04/Dateline-SE_Spring15.pdf) ("A patient receiving medical care fraudulently can lead to the real patient receiving the wrong blood type, prescription, or even being misdiagnosed at a later time.").

<sup>40</sup> N.D. Cent. Code § 51-30.

<sup>41</sup> William Elser, *Recent Updates to State Data Breach Notification Laws in New Mexico, Tennessee, Virginia*, Lexology (May 1, 2017), <https://www.lexology.com/library/detail.aspx?g=b02a15ac-a3c3-460d-bc5e-1d29778c4e59> ("New Mexico's new law defines 'personal identifiable information' consistently with most other states, and joins a growing number of states that have broadened the definition to include 'biometric data,' which is defined to include 'fingerprints, voice print, iris or retina patterns, facial characteristics or hand geometry.'").

<sup>42</sup> Conn. Gen. Stat. § 38a-999b.

<sup>43</sup> NMSA §§ 57-12C-2; 57-12C-4.

weakening the protections that consumers currently enjoy. I urge this Committee not to approve such a bill.

**C. Federal Legislation Should Provide Flexibility to Adjust to New and Changing Threats**

Relatedly, a number of legislative proposals that have been advanced in the past would not provide the necessary flexibility to account for changing technology and information practices. Consumers are constantly encountering new types of threats as the information landscape evolves and creative attackers come up with new ways to exploit breached data. States are responding to developing threats affecting their residents by adjusting data security and breach notification protections as changing circumstances require, including by adding new categories of protected information such as medical information and biometric data.

We can't always forecast the next big threat years in advance, but unfortunately, we know that there will be one. For example, there are now multiple services that allow customers to upload photographs of physical car keys and house keys to the cloud, then order copies of those keys through an app, over the Web, or at key-cutting kiosks located at brick-and-mortar stores.<sup>44</sup> Will malicious attackers begin targeting photographs of keys to victims' homes? It might be too early to tell, but if they do, companies that collect and maintain that information ought to notify their customers, and the law ought to be able to be quickly adjusted to make sure that they do, without Congress having to pass another bill first.

The flexibility we need could be built into federal legislation in one of two ways. First, Congress could limit preemption in a manner that allows states to continue to establish standards for categories of information that

---

<sup>44</sup> Andy Greenberg, *The App I Used to Break into My Neighbor's Home*, WIRED (Jul. 25, 2014), <http://www.wired.com/2014/07/keyme-let-me-break-in/>; Sean Gallagher, *Now You Can Put Your Keys in the Cloud—Your House Keys*, Ars Technica (Mar. 20, 2015), <http://arstechnica.com/information-technology/2015/03/now-you-can-put-your-keys-in-the-cloud-your-house-keys/>.

fall outside the scope of federal protection as, for example, states have recently done with medical information and biometric data. Alternatively, Congress could establish agency rulemaking authority to redefine the category of protected information as appropriate to meet new threats. The Committee should not advance any data security and breach notification legislation that is not adaptable in one of these ways.

**D. Federal Legislation Should Include Enforcement Authority for State Attorneys General**

In the event the Committee ultimately approves a bill that preempts state data security and breach notification laws, the Committee should ensure that any such bill nevertheless includes both a requirement to notify, and an enforcement role for, state attorneys general. At a minimum, state attorneys general should have the authority to bring actions in federal court under the new federal standard.

State attorneys general play a critical role in policing data security and guiding breach notification to match the needs of their own residents. In addition, state attorneys general are essential in conducting ongoing monitoring after a breach has occurred to help protect residents from any aftermath, especially where small data breaches are concerned. According to the Massachusetts State Attorney General's Office, Massachusetts alone saw 2,314 data breaches reported in 2013, 97% of which involved fewer than 10,000 affected individuals.<sup>45</sup> Each data breach affected, on average, 74 individuals.<sup>46</sup>

Federal agencies are well equipped to address large data security and breach notification cases, but could be overwhelmed if they lose the

---

<sup>45</sup> Testimony of Sara Cable before the House Energy & Commerce Committee Subcommittee on Commerce, Manufacturing, and Trade regarding the Data Security and Breach Notification Act of 2015, *available at* <http://docs.house.gov/meetings/IF/IF17/20150318/103175/HHRG-114-IF17-Wstate-CableS-20150318.pdf>.

<sup>46</sup> *Id.*

complementary consumer protection support of state attorneys general in thousands of small cases each year. To ensure that consumers receive the best protection they possibly can—even when they are among a small handful of individuals affected by a breach—state attorneys general must be given the ability to help enforce any new federal standard.

**E. Federal Legislation Narrowly Designed for Data Security and Breach Notification Should Be Crafted Not to Preempt a Wide Range of Privacy and General Consumer Protection Laws**

Federal legislation also must be careful not to invalidate a wide range of existing consumer protections, including provisions that are at times used to enforce data security, but that are also used to provide other consumer or privacy protections. For example, the preemption provisions of some legislative proposals we have seen extend only to securing information from unauthorized access,<sup>47</sup> but as a practical matter, it will be exceedingly difficult to draw the line between information security and breach notification on the one hand, and privacy and general consumer protection on the other.

Generally speaking, “privacy” has to do with how information flows, what flows are appropriate, and who gets to make those determinations. Data or information “security” refers to the tools used to ensure that information flows occur as intended. When a data breach occurs, both the subject’s privacy (their right to control how their information is used or

---

<sup>47</sup> H.R. 2205 would preempt requirements or prohibitions imposed under state law with respect to “safeguard[ing] information relating to consumers from (A) unauthorized access; and (B) unauthorized acquisition.” H.R. 1770 would preempt state law “relating to or with respect to the security of data in electronic form or notification following a breach of security.” It would supersede several sections of the Communications Act insofar as they “apply to covered entities with respect to securing information in electronic form from unauthorized access, including notification of unauthorized access to data in electronic form containing personal information.”

shared) and information security (the measures put in place to facilitate and protect that control) are violated.

Privacy and security are thus distinct concepts, but they go hand in hand. From the consumer's perspective, a data breach that results in the exposure of her call records to the world is a terrible violation of her privacy. But the cause of the privacy violation may be a breakdown in security.

Accordingly, agencies enforcing against entities for security failures cite both privacy and security at the same time. For example, in the complaint it filed in June 2010 against Twitter for failing to implement reasonable security, the Federal Trade Commission argued that Twitter had "failed to provide reasonable and appropriate security to: prevent unauthorized access to nonpublic user information *and honor the privacy choices exercised by its users in designating certain tweets as nonpublic.*"<sup>48</sup>

Not only does enforcement often address privacy and security simultaneously, but many laws that protect consumers' personal information could also be thought of in terms of both privacy and security. For example, in California, the Song-Beverly Credit Card Act prohibits retailers from recording any "personal identification information" of a credit cardholder in the course of a transaction.<sup>49</sup> In Connecticut, Section 42-470 of the General Statutes prohibits the public posting of any individual's Social Security number.<sup>50</sup> These laws could be framed as both privacy and data security laws. State-level general consumer protection laws prohibiting unfair and deceptive trade practices (sometimes known as "mini-FTC Acts") are also used to enforce both privacy and security.

Because each of these examples highlights a circumstance where privacy and security regulations are blended together, legislative proposals that may intend to leave intact privacy laws could nevertheless unintentionally eliminate privacy-oriented consumer protections that have a

---

<sup>48</sup> *Twitter, Inc.*, Complaint, para. 11 (2010), available at <https://www.ftc.gov/sites/default/files/documents/cases/2010/06/100624twittercmpt.pdf> (emphasis added).

<sup>49</sup> Cal. Civ. Code § 1747.08.

<sup>50</sup> Conn. Gen. Stat. § 42-470.

data security aspect. Congress should therefore carefully tailor the scope of preemption in any data security and breach notification legislation it advances to avoid invalidating numerous privacy protections.

### **Conclusion**

I am grateful for the Committee's attention to this important issue, and for the opportunity to present this testimony.

**NCLC**

NATIONAL  
CONSUMER  
LAW  
CENTER\*

Advancing Fairness  
in the Marketplace for All

**Testimony before the  
U.S. HOUSE OF REPRESENTATIVES COMMITTEE ON FINANCIAL SERVICES**  
regarding

“Examining the Equifax Data Breach”

October 25, 2017

**Chi Chi Wu**

Staff Attorney

**National Consumer Law Center**

7 Winthrop Square, 4th Fl.

Boston, MA 02110

617-542-8010

[cwu@nclc.org](mailto:cwu@nclc.org)



Testimony of Chi Chi Wu, National Consumer Law Center  
Before the U.S. House of Representatives Committee on Financial Services  
regarding  
“Examining the Equifax Data Breach”  
October 25, 2017

**INTRODUCTION AND SUMMARY**

Mr. Chairman, Ranking Member Waters, and Members of the Subcommittee, thank you for inviting me to testify today regarding the Equifax data breach. I offer my testimony here on behalf of the low-income clients of the National Consumer Law Center.<sup>1</sup>

NCLC has long advocated for stronger reforms to ensure accuracy and fairness in the U.S. credit reporting system. We have testified many times before Congress, including before this Committee, on the need for reform of the credit reporting system to address issues such as unacceptable error rates, the travesty of the automated dispute system used by the credit reporting agencies or “CRAs,” the unfair impact of medical debt on credit reports, and the problems with use of credit reports for employment purposes.<sup>2</sup>

In fact, on the day that Equifax announced the data breach, NCLC was testifying against six anti-consumer bills before the Subcommittee on Financial Institutions and Consumer Credit. Ironically, one of the bills under consideration that day (H.R. 2359, the FCRA Liability Harmonization Act) would eliminate punitive damages and limit class action damages under the Fair Credit Reporting Act (FCRA), dramatically reducing the consequences when Equifax and other credit reporting agencies violate the FCRA. We understand that Representative Loudermilk, the lead sponsor of H.R. 2359, has said he will table the bill for now,<sup>3</sup> but we stand ready to vigorously oppose it again if it is moved forward.

---

<sup>1</sup> The National Consumer Law Center is a nonprofit organization specializing in consumer issues on behalf of low-income people. We work with thousands of legal services, government and private attorneys, as well as community groups and organizations, from all states who represent low-income and elderly individuals on consumer issues. As a result of our daily contact with these advocates, we have seen many examples of the damage wrought by abuses from credit reporting agencies from every part of the nation. It is from this vantage point that we supply these comments. *Fair Credit Reporting* (8th ed. 2013) is one of the eighteen practice treatises that NCLC publishes and annually supplements. This testimony was written by Chi Chi Wu, with assistance from Lauren Saunders of NCLC.

<sup>2</sup> See, e.g., An Overview of the Credit Reporting System: Hearing Before the Subcomm. on Fin. Inst. and Consumer Credit of the H. Comm. on Fin. Servs., 113th Congr. (2014) (testimony of Chi Chi Wu); Use of Credit Information beyond Lending: Issues and Reform Proposals: Hearing Before the Subcomm. on Fin. Inst. and Consumer Credit of the H. Comm. on Fin. Servs., 113th Congr. (2010) (testimony of Chi Chi Wu).

<sup>3</sup> Zachary Warmbrodt, Finance industry's deregulation drive faces new threat with Equifax, Politico, Sept. 13, 2017, at <http://www.politico.com/story/2017/09/13/equifax-finance-industry-deregulation-242634> (“The congressman instructed the committee that ‘he would like to see no further action on H.R. 2359, pending a full and complete investigation into the Equifax breach,’ according to Loudermilk spokeswoman Shawna Mercer”).

### I. The Equifax breach

By now, we are all too familiar with the shocking facts of the Equifax data breach, in which thieves were able to steal the Social Security numbers, dates of birth, and other sensitive information for a mind-boggling 145.5 million Americans. This means half of the US population and nearly three-quarters of the consumers with active credit reports are now at risk of identity theft due to one of the worst – if not the worst – breaches of consumer data in American history. These Americans are at risk of having false new credit accounts, phony tax returns, and even spurious medical bills incurred in their good names.

We know about Equifax's incompetent failure to install a simple cybersecurity patch that led to the massive hack. We have seen Equifax repeatedly bungle its response to the data breach, including inserting a forced arbitration clause in the product it initially offered to breach victims for remediation,<sup>4</sup> tweeting out a fraudulent link to a website that spoofed Equifax's own website for breach victims,<sup>5</sup> and having completely insufficient website and telephone resources resulting on long delays for victims seeking information or freezes.<sup>6</sup>

This horrifying data breach has made Americans aware of the anomalous nature of the credit reporting industry. The companies serve a critically important function in the U.S. economy and in the financial lives of Americans. A good credit history is necessary for consumers to obtain credit, and to have that credit be fairly priced. Credit reports are also used by other important decisionmakers, such as insurers, landlords, utility providers, and unfortunately, even employers. Thus, it is no exaggeration to say that a credit history can make or break a consumer's finances.

Yet credit reporting agencies are entirely private companies that are publicly traded, which means their highest duty is to shareholder profit. Furthermore, consumers do not have any leverage over these private companies, unlike most other industries, because market forces do not apply to this industry.

The American consumer is not the customer, but rather the commodity, of the credit reporting agencies. We have no choice but to have our data fed to these companies. We cannot vote with our feet or our purse strings – we cannot choose to avoid Equifax even after this terrible hack if we want a credit card, a car loan, or a mortgage. When late night hosts make jokes about this awful situation,<sup>7</sup> we know this is a problem that everyone is paying attention to.

---

<sup>4</sup> See Section IV, below.

<sup>5</sup> Alfred Ng, Equifax Sends Breach Victims to Fake Support Site, CNET.com, Sept. 20, 2017, at [www.cnet.com/news/equifax-twitter-fake-support-site-breach-victims/](http://www.cnet.com/news/equifax-twitter-fake-support-site-breach-victims/).

<sup>6</sup> Rob Lieber, Finally, Some Answers From Equifax to Your Data Breach Questions, N.Y. Times, Sept. 14, 2017, available at [www.nytimes.com/2017/09/14/your-money/equifax-answers-data-breach.html](http://www.nytimes.com/2017/09/14/your-money/equifax-answers-data-breach.html) (“Some people are waiting until the middle of the night to try to use Equifax's security freeze website and even failing then to get through. It's like trying to get Bruce Springsteen tickets, except nobody wants to see this particular show”).

<sup>7</sup> See, e.g., John Oliver, Equifax: Last Week Tonight with John Oliver, Oct. 15, 2017, available at [www.youtube.com/watch?v=mPjgRKW\\_Jmk](http://www.youtube.com/watch?v=mPjgRKW_Jmk); Stephen Colbert, Equifax Just Equi-F'ed Everyone, The Late Show with Stephen Colbert, Sept. 21, 2017, available at [www.youtube.com/watch?v=Ly1Ed5QVkyC](http://www.youtube.com/watch?v=Ly1Ed5QVkyC).

In addition to the lack of market forces to rein them in, the credit reporting agencies were also insufficiently regulated until recently. Until 2012, their primary regulator was the beleaguered Federal Trade Commission (FTC), which only had the power to take enforcement action when something went wrong and which was outstaffed and outgunned. Private attorneys can sue under the FCRA, but they generally cannot seek injunctive relief,<sup>8</sup> so the companies can pay off the lawsuits as a cost of doing business and not fix their systems.

## II. A culture of impunity, arrogance, and exploitation

Due to this insufficient regulation and the lack of consumer choice, the credit reporting agencies have grown up in a culture of impunity, arrogance, and exploitation. For decades, they have abused consumers, cut corners in personnel and systems, and failed to invest in measures that would promote accuracy or handle disputes properly. Their idea of a dispute system was a travesty of automation, converting painstakingly written consumer disputes and supporting documentation into two- or three-digit codes and sending only those codes to the creditor or debt collector (the “furnisher”) that provided the erroneous information. After the furnisher responded, the credit reporting agencies’ main response was to repeat or “parrot” whatever the furnisher claimed. The CRAs always took the side of the furnisher, like a judge that always sides with the defendant. And they often spent minimal resources on disputes -- at one point, Equifax paid a mere \$0.57 per dispute letter to a Philippines-based vendor to handle disputes.<sup>9</sup>

The credit reporting agencies also have accuracy rates that are unacceptable. The definitive FTC study on credit reporting errors found that 1 in 5 consumers have verified errors in their credit reports, and 1 in 20 consumers have errors so serious they would be denied credit or need to pay more for it.<sup>10</sup> It is no surprise then that the three credit reporting agencies are often the top three most complained-about companies to the Consumer Financial Protection Bureau (Consumer Bureau), with the vast majority of complaints involving incorrect information on consumers’ credit reports.<sup>11</sup>

Furthermore, these problems with accuracy stem fundamentally from a culture where compliance and quality control take a back seat to profits and marketing. A Consumer Financial Protection Bureau report documenting its supervision efforts over the credit reporting agencies noted major deficiencies at the CRAs, such as:<sup>12</sup>

<sup>8</sup> National Consumer Law Center, Fair Credit Reporting § 11.12 (8th ed. 2013), *updated at* [www.nclc.org/library](http://www.nclc.org/library).

<sup>9</sup> Chi Chi Wu, National Consumer Law Center, Automated Injustice: How a Mechanized Dispute System Frustrates Consumers Seeking to Fix Errors in Their Credit Reports (Jan. 2009), at 32, *available at* [www.nclc.org/images/pdf/pr-reports/report-automated\\_injustice.pdf](http://www.nclc.org/images/pdf/pr-reports/report-automated_injustice.pdf).

<sup>10</sup> Federal Trade Comm’n Report to Congress Under Section 319 of the Fair and Accurate Credit Transactions Act of 2003 (Dec. 2012).

<sup>11</sup> *See, e.g.*, Consumer Financial Protection Bureau, Monthly Complaint Report, Vol. 21, March 2017, *available at* [https://s3.amazonaws.com/files.consumerfinance.gov/f/documents/201703\\_cfpb\\_Monthly-Complaint-Report.pdf](https://s3.amazonaws.com/files.consumerfinance.gov/f/documents/201703_cfpb_Monthly-Complaint-Report.pdf).

<sup>12</sup> Consumer Financial Protection Bureau, Supervisory Highlights Consumer Reporting Special Edition, Issue 14 (Mar. 2, 2017), *available at* [http://files.consumerfinance.gov/f/documents/201703\\_cfpb\\_Supervisory-Highlights-Consumer-Reporting-Special-Edition.pdf](http://files.consumerfinance.gov/f/documents/201703_cfpb_Supervisory-Highlights-Consumer-Reporting-Special-Edition.pdf).

- No programs to test the accuracy of credit reports that the CRAs produced, prompting Consumer Bureau Director Richard Cordray to remark “we were surprised to find that [the CRAs’] quality control systems were either rudimentary or virtually non-existent.”<sup>13</sup>
- Insufficient monitoring and re-vetting of furnishers to ensure they were continuing to meet their legal and other obligations. Furnishers were rarely provided with feedback regarding data quality, and were sometimes charged fees for data-quality reports.
- Deficiencies regarding dispute handling, not only in conducting cursory reviews as discussed above, but failing to consistently notify furnishers of disputes and to describe the results of dispute investigations in FCRA-mandated notices to consumers.

From our years of experience with the credit reporting agencies, and as demonstrated by the Consumer Bureau’s report, it appears their culture is to cut corners and to underinvest in compliance management and quality control. *A data company that underinvests in accuracy and compliance is likely to be the same company that will underinvest in information security.* The yawning gaps in data security at Equifax probably stem from the same attitude of trying to see how much it could reduce costs and maximize profits. An emphasis on profits over doing the job right is what we believe contributed to this massive data breach at Equifax. Furthermore, Equifax is not alone, as we believe that the other two big credit reporting agencies (Experian and TransUnion) have similar cultures.

### III. The credit reporting agencies promote their own products instead of credit freezes

This attitude of impunity has also manifested itself in the credit reporting agencies’ aggressive marketing of credit monitoring as the preferred response to data breaches, instead of offering the far more effective measure of credit freezes, also known security freezes. Credit monitoring is not as effective as security freezes because it only informs consumers after the fact when there has been an attempt to open a fraudulent new account using the consumer’s personal information— the proverbial shutting the barn door after the horse has left. A security freeze prevents the consumer’s stolen information from being used by thieves in the first place.

The reason that credit reporting agencies promote credit monitoring in response to breaches is simple: the CRAs want to establish credit monitoring as the automatic response when a consumer is worried about identity theft. In addition to the revenues from businesses and government agencies, the real pot of gold is when consumers sign up for the paid subscription version of credit monitoring and ID theft prevention products, which cost \$5 to \$30 per month, generating a whopping \$3 billion in profits in 2015 and 2016.<sup>14</sup>

<sup>13</sup> Prepared Remarks of Consumer Financial Protection Bureau Director Richard Cordray at the Consumer Advisory Board Meeting, Mar. 2, 2017, available at <https://www.consumerfinance.gov/about-us/newsroom/prepared-remarks-cfpb-director-richard-cordray-consumer-advisory-board-meeting-march-2017/>

<sup>14</sup> Government Accountability Office, Identity Theft Services: Services Offer Some Benefits but Are Limited in Preventing Fraud, GAO-17-254, March 17, at 5, *available at* [www.gao.gov/assets/690/683842.pdf](http://www.gao.gov/assets/690/683842.pdf). Not all of \$3 billion went to the three primary nationwide CRAs, as there are dozens of companies that offer identity theft prevention products. However, identity theft prevention services usually include a credit monitoring component. For example, the GAO noted that all

In fact, the practice of promoting credit monitoring subscriptions was so ingrained that Experian actually refused to provide free credit freezes when it experienced its own data breach. In October 2015, Experian announced that it had experienced a breach in which the Social Security numbers and other personal data of 15 million T-Mobile customers was stolen. Consumer advocates urged Experian to provide free credit freezes to consumers whose information was stolen.<sup>15</sup> Not only did Experian refuse to officially respond to the consumer advocates, an Experian official accidentally copied consumer advocates on an email sent to Experian North America's CEO stating:

"This is a predictable response from this group. The precedent set for offering free freezes would haunt all beaches going forward. Doing as they request on either count will not satiate their hatred for Experian.

"We should respond with a well articulated letter regarding why a credit freeze is not a credible response for most people. Fraud alerts and monitoring is adequate. It would also allow us to explain that the data won't likely be used, and that we have remediation experts available to help if it is.

"We could turn our response into a good PR approach if done right."

A copy of this email is attached as Attachment A.

Experian deliberately made a choice not to promote the most effective measure against identity theft to consumers who had been victimized by a breach of its own doing. Experian put consumers it had already harmed at risk of identity theft solely to avoid jeopardizing its lucrative credit monitoring business for future breaches.

Indeed, in this most recent breach, Equifax's initial response was to offer one free year of its credit monitoring and identity theft prevention product.<sup>16</sup> But because of intense media scrutiny generated by the massive scale of this breach, consumer advocates and public officials were finally able to get the message out on a large scale that consumers should place credit freezes on their accounts to protect themselves against identity theft. As a result, Equifax initially agreed to provide free credit freezes until November 21, 2017, then to January 31, 2018.<sup>17</sup>

However, even after this massive breach and the intense scrutiny surrounding it, the culture of impunity still remains with the credit reporting agencies. This time around, the credit reporting

---

but 3 of the 26 identity theft service providers it reviewed provided some level of credit monitoring. Thus any provider that is not a CRA must contract with a CRA to provide access to consumer credit reports. *Id.* at 9. Consequently, the CRAs make money even when their competitors sell a subscription product that includes credit monitoring.

<sup>15</sup> Letter from Consumer Advocates to Experian and T-Mobile re: Data Breach, Oct. 2, 2015, *available at* [www.nclc.org/images/pdf/credit\\_reports/letter-experian-data-breach-oct2015.pdf](http://www.nclc.org/images/pdf/credit_reports/letter-experian-data-breach-oct2015.pdf).

<sup>16</sup> Press Release, Equifax Announces Cybersecurity Incident Involving Consumer Information, Sept. 7, 2017, *available at* <https://investor.equifax.com/news-and-events/news/2017/09-07-2017-213000628>.

<sup>17</sup> FTC, Free credit freezes from Equifax, Sept. 19, 2017 (updated Oct. 5, 2017 to reflect new January 31, 2018 date), *available at* [www.consumer.ftc.gov/blog/2017/09/free-credit-freezes-equifax](http://www.consumer.ftc.gov/blog/2017/09/free-credit-freezes-equifax).

agencies are promoting credit “locks” instead of credit freezes. Indeed, in its website, TransUnion heavily steers consumers toward its free credit “lock” product and away from freezes, comparing locks and freezes in a very biased manner. For example, TransUnion notes that:<sup>18</sup>

- Lock - You want instant independent control over access to your credit information
- Freeze - You'd rather have TransUnion control access to your credit information

What Transunion neglects to inform consumers is that:

- The “lock” is part of TransUnion’s TrueIdentity product. Consumers must agree to an arbitration clause as part of the TrueIdentity product.<sup>19</sup>
- TransUnion generates profits by sending targeted advertising to consumers as part of this product. While this fact by itself is not objectionable, TransUnion fails to point out that this is a drawback to this product in comparison to a security freeze.
- Most importantly, a security freeze is mandated by state law, and there is legal liability if TransUnion fails to comply with the terms of state law. A lock is simply a product offered by TransUnion, and if something goes wrong, the consumer’s only remedies are perhaps for breach of contract or unfair practices.

Equifax has announced that it will be offering a free credit lock product for life.<sup>20</sup> It is unclear whether Equifax’s credit lock will be associated with an arbitration clause. During testimony before both the House and Senate, former CEO Rick Smith did state there would be no advertising as part of the product. However, he heavily promoted the credit lock product as superior to security freezes without noting the potential drawbacks.

Finally, at least TransUnion and Equifax are offering their lock products without charging a fee. Experian is not offering anything for free.<sup>21</sup> And note that TransUnion or Equifax could decide to stop offering free credit locks at any point, perhaps when the media attention is no longer focused on them, and consumers would have little recourse.

There should be a right to free security freezes for all consumers. After all, this is OUR information in the credit reporting agencies’ database, from which they are making billions in profits. Consumers should at least have the control to shut off access to their own information when they are not actively seeking credit. Ideally, a security freeze should be placed on credit reports by default, and access should be turned off until the consumer decides to turn it on.

<sup>18</sup> TransUnion, Locking Your Credit Report, at [www.transunion.com/credit-freeze/place-credit-freeze2](http://www.transunion.com/credit-freeze/place-credit-freeze2) (viewed Oct. 19, 2017).

<sup>19</sup> TransUnion, Service Agreement, at [www.trueidentity.com/legal/service-agreement](http://www.trueidentity.com/legal/service-agreement) (viewed October 21, 2017).

<sup>20</sup> Paulino do Rego Barros Jr., On Behalf of Equifax, I’m Sorry, Wall St. J., Sept. 27, 2017, available at [www.wsj.com/articles/on-behalf-of-equifax-im-sorry-1506547253](http://www.wsj.com/articles/on-behalf-of-equifax-im-sorry-1506547253).

<sup>21</sup> Ron Lieber, Equifax Calls for Free Credit Locks. Experian’s Reply? Nope., New York Times, Oct. 4, 2017, available at [www.nytimes.com/2017/10/04/your-money/equifax-experian-credit-locks.html](http://www.nytimes.com/2017/10/04/your-money/equifax-experian-credit-locks.html).

#### IV. Use of Forced Arbitration by Credit Reporting Agencies

The credit reporting agencies' culture of impunity is aided and abetted by their use of forced arbitration clauses. Equifax was slow to alert the public to the data breach, but quick to protect itself by attempting to take away consumers' day in court. Buried in the fine print of the website it set up to offer free credit monitoring was a forced arbitration clause and class action ban purporting to apply to any controversy "relating in any way to Your relationship with Equifax" and to be interpreted in "the broadest possible" manner. Equifax eventually relented and removed the clause under intense pressure.<sup>22</sup> But former Equifax CEO Rick Smith, when testifying before the Senate Banking Committee on October 4, admitted that Equifax uses arbitration clauses in other consumer products.<sup>23</sup> Furthermore, it should not be up to the wrongdoer to decide voluntarily if consumers get access to justice, and it should not happen only when a problem is massive enough to generate intense publicity.

Experian and TransUnion also include forced arbitration clauses with class action bans in their products. Experian includes a forced arbitration clause in ProtectMyID.<sup>24</sup> As mentioned above, TransUnion includes one in its TrueIdentity product. The Seventh Circuit criticized TransUnion for one of its arbitration clauses, stating that the company "actively misleads consumers" into thinking that clicking "I Accept" merely authorized TransUnion to obtain information needed to get a credit score, not to force them to give up their day in court.<sup>25</sup>

TransUnion should know the power of class actions to obtain relief for those wrongfully abused, given that it recently lost a lawsuit for carelessly mismatching innocent consumers with suspected criminals and terrorists with similar names on a government watch list. The jury was so appalled by TransUnion's conduct that it ordered the company to pay \$60 million (\$7,337 for each of the 8,185 class members). Military personnel serving our country abroad were among those mislabeled as potential terrorists or criminals.<sup>26</sup>

A new Consumer Bureau rule will stop these abuses by prohibiting financial companies from putting forced arbitration clauses with class action bans in the fine print of contracts.<sup>27</sup> The rule applies to companies providing credit reports, credit scores, credit monitoring and other services provided to consumers based on information in the consumer's file. But the House of Representatives has voted to repeal the rule and the Senate is considering following suit. This is despite the fact that a recent phone survey conducted by a Republican firm found that, in the

<sup>22</sup> Diane Hembree, *Consumer Backlash Spurs Equifax To Drop 'Ripoff Clause' In Offer To Security Hack Victims*, *Forbes*, *available at* [www.forbes.com/sites/dianahembree/2017/09/09/consumer-anger-over-equifax-ripoff-clause-in-offer-to-security-hack-victims-spurs-policy-change/#2d2a93ef6e7e](http://www.forbes.com/sites/dianahembree/2017/09/09/consumer-anger-over-equifax-ripoff-clause-in-offer-to-security-hack-victims-spurs-policy-change/#2d2a93ef6e7e).

<sup>23</sup> Former Equifax CEO Faces Congress, *Wall St. J.*, Oct. 4, 2017, *available at* <https://www.wsj.com/livecoverage/equifax-hack-hearing-1003>.

<sup>24</sup> Experian, *ProtectMyID® Membership Agreement*, Sept. 1, 2015, *at* <http://www.protectmyid.com/terms> (viewed Oct. 21, 2017).

<sup>25</sup> *Sgouros v. Transunion Corp.*, 817 F.3d. 1029, 1035 (7th Cir. 2016).

<sup>26</sup> James A. Francis, *Don't Strip Service Members of Their Right to Join Class-Action Lawsuits*, *Morning Consult*, Oct. 19, 2017, *available at* <https://morningconsult.com/opinions/service-members-military-arbitration-fraud-class-action/>.

<sup>27</sup> *See* Consumer Financial Protection Bureau, *New protections against mandatory arbitration*, July 20, 2017, *at* [www.consumerfinance.gov/arbitration-rule](http://www.consumerfinance.gov/arbitration-rule).

wake of Equifax's massive data breach, the Consumer Bureau's rule has widespread bipartisan support ranging from 64% among Republicans to 74% among Democrats.<sup>28</sup>

#### V. The need for close supervision

With respect to accuracy and dispute handling, we are finally starting to see modest improvements in the credit reporting agencies. In 2012, American consumers finally got a regulator with the tools, focus, and resources to force the credit reporting agencies to improve their systems – the Consumer Financial Protection Bureau (Consumer Bureau). The Consumer Bureau has started supervising the CRAs by examining their policies, procedures, compliance systems, and employee training. This supervision has begun to start paying by moving the needle on accuracy and dispute issues.<sup>29</sup>

However, Consumer Bureau's supervision is missing a critical element – *it has no mandate to supervise for data security*. When the Dodd-Frank Act created the Consumer Bureau, Congress decided to shift most of the FCRA authority to this new agency, but to keep the identity theft and data security provisions of the FCRA with the FTC. And the major federal law governing data security for the credit reporting agencies – the Gramm Leach Bliley Act – specifically excludes Consumer Bureau from jurisdiction over its data security provisions. See 15 U.S.C. §§ 6801(b), 6805(b)(1). While the Consumer Bureau could potentially supervise for data security under other authority, such as the prohibition against unfair, abusive or deceptive practices under Section 1031 of the Consumer Financial Protection Act, the lack of a clear mandate means that the supervision priority has been to focus on issues for which the Bureau does have a mandate – accuracy and dispute handling.

At the time Dodd-Frank was passed, this division of authority might have made sense. But it has resulted in terrible consequences. The FTC has no supervision authority to investigate proactively what is going on inside the credit reporting agencies. The FTC can only react after the fact to this data breach by taking enforcement action. It could not have prevented this tragedy, because it could never get inside the guts of the credit reporting companies to make sure their data security was adequate and compliant.

We believe the Gramm-Leach-Bliley data security authority should be transferred over to the Consumer Financial Protection Bureau. The Bureau can make data security part of its current supervisory efforts and force the companies to fix their systems before there is another terrible breach. The Consumer Bureau has the infrastructure and resources to dig deep into the procedures and policies of these companies on data security. We need the most effective regulator – the only one examining the credit reporting agencies – to be in charge of making sure the CRAs properly invest in data security.

<sup>28</sup> Sylvan Lane, GOP polling firm: Bipartisan support for consumer bureau arbitration rule, The Hill, Oct. 5, 2017, available at <http://thehill.com/policy/finance/354143-gop-polling-firm-finds-bipartisan-support-for-consumer-bureau-arbitration-rule>.

<sup>29</sup> In addition, a settlement obtained by a multistate group of Attorneys General with the credit reporting agencies also requires the agencies to improve dispute handling and accuracy procedures. Assurance of Voluntary Compliance/Assurance of Voluntary Discontinuance, In the Matter of Equifax Info. Serv. L.L.C., Experian Info. Solutions, Inc., and TransUnion L.L.C. (May 20, 2015).



#### VI. Necessary reforms

Congress should adopt some fundamental immediate reforms in response to the Equifax data breach:

- **Consumers should not be forced to pay for security freezes under any circumstances, much less after they have been victimized by a data breach.** That's why we have supported several bills to mandate free security freezes. Free security freezes are also a component of H.R. 3755, the Comprehensive Credit Reporting Reform Act, sponsored by Ranking Member Maxine Waters.
- **The Consumer Financial Protection Bureau should be given the authority over the data security standards under the Gramm Leach-Bliley Act and the FCRA so that it has a clear mandate to supervise the credit reporting agencies regarding this area.**
- **The Internal Revenue Service (IRS) should make identity protection personal identification numbers (PINs) available to everyone.** The Equifax breach has put 145.5 million Americans at risk of other types of identity theft, such as tax refund identity theft, in which crooks file phony tax returns using consumers' names and identifiers, then steal the refund. The only method to prevent tax identity theft is an Identity Protection PIN from the IRS, but the IRS only makes PINs available to prior victims of identity theft and to consumers in Florida, Georgia, and the District of Columbia. Thus, we have urged IRS to make Identity Protection PINs available to all affected breach victims<sup>30</sup> and Congress should make a similar demand.
- **Congress should enact wider reforms of the credit reporting industry.** This data breach has very much highlighted the problems with and abuses by credit reporting agencies, and these should all be addressed. That is why we strongly support H.R. 3755, the Comprehensive Credit Reporting Reform Act, and we thank Ranking Member Waters for introducing it.

Finally, we agree with commentators who have suggested that a new paradigm for credit reporting might be necessary. We want to make clear that we are not urging the elimination of Equifax, because frankly the other two credit reporting agencies are as equally flawed. Indeed, Equifax has exhibited some remorse and apologized, but as demonstrated above, TransUnion and Experian have not changed their attitude at all and are still engaged in less than forthright tactics.

Some commentators have urged that credit reporting be a public function, or that we nationalize the CRAs. Those ideas are worth exploring and studying. For example, credit reporting could be a function of government-sponsored enterprises, similar to the role of Fannie Mae and Freddie Mac in the mortgage market.

---

<sup>30</sup> Letter from consumer and tax attorneys urging IRS to make Identity Theft PINs available to all taxpayers, Sept. 21, 2017, *available at* [www.nclc.org/images/pdf/credit\\_reports/irs-ltr-re-efx-breach.pdf](http://www.nclc.org/images/pdf/credit_reports/irs-ltr-re-efx-breach.pdf).

Conclusion

The massive theft of sensitive personal information for half of all Americans demands a real and meaningful response by Congress. Some media outlets have speculated Congress will do nothing more than make public displays of outrage at Equifax. We urge this Committee to prove them wrong.

Thank you very much for the opportunity to testify today. I would be happy to answer any questions.

ATTACHMENT ANCLC<sup>®</sup>

Chi Chi Wu &lt;ccwu@nclc.org&gt;

**Re: Consumer Groups Call on Experian and T-Mobile to Provide Free Security Freezes to Hacked Customers**

1 message

**Hadley, Tony**

Fri, Oct 2, 2015 at 2:48 PM

To: Chi Chi Wu

Cc: "John.Legere, "Boundy, Craig"

This is a predictable response from this group. The precedent set for offering free freezes would haunt all beaches going forward. Doing as they request on either count will not satiate their hatred for Experian.

We should respond with a well articulated letter regarding why a credit freeze is not a credible response for most people. Fraud alerts and monitoring is adequate. It would also allow us to explain that the data won't likely be used, and that we have remediation experts available to help if it is.

We could turn our response into a good PR approach if done right.

Thoughts?

I would be happy to draft an initial response.

Tony

Sent from my iPhone

On Oct 2, 2015, at 11:15 AM, Chi Chi Wu wrote:

Dear Mr. Boundy and Mr. Legere: Please see the attached letter, the text of which is also copy-pasted below.

October 2, 2015

Craig Boundy

John Legere

CEO

CEO

Experian North America

T-Mobile US

Dear Mr. Boundy and Mr. Legere:

The undersigned consumer advocacy and labor groups write to you regarding the recent announcement that there has been a massive security breach of T-Mobile customer data from Experian. We understand from media reports that over 15 million consumers may have had their sensitive personal information, including Social Security Numbers and other identifying numbers (such as driver's license information), stolen by hackers.

The media stories also report that Experian and T-Mobile are offering free credit monitoring for two years in response to the security breach. We are writing to urge that, in addition, Experian and T-Mobile should offer *free security freezes* to all affected customers, for all three major credit bureaus. Otherwise, affected consumers could be charged up to \$15 per credit bureau.

<https://mail.google.com/mail/u/0/?ui=2&ik=fc55df44f1&jsver=BNKYf1ymS-0.en.&view=pt&q=tony.hadley%40experian.com&q=true&search=query&th=...> 1/2

As you know, a security freeze is the most effective measure against identity theft involving the opening of new credit accounts, and is certainly advised here given the highly sensitive information that was stolen. Credit monitoring only informs consumers after the fact when there has been an attempt to open a fraudulent new account using the consumer's personal information— the proverbial shutting the barn door after the horse has left. A security freeze prevents the consumer's stolen information from being used by thieves in the first place.

Finally, we urge that Experian remove its mandatory arbitration provision from its credit monitoring agreement for the affected customers, and for all customers of its credit monitoring products. It's bad enough that Experian has allowed hackers to infiltrate its computer systems; to then slip in a provision in the credit monitoring agreement that deprives these victimized consumers of their legal remedies against Experian is unconscionable.

If you have any questions about this letter, please contact Chi Chi Wu at 617-542-8010 or [cwu@nclc.org](mailto:cwu@nclc.org).

Sincerely,

National Consumer Law Center (on behalf of its low-income consumers)

Communications Workers of America, CWA

Consumer Action

Center for Digital Democracy

Center for Economic Justice

National Association of Consumer Advocates

U.S. PIRG

Woodstock Institute

Housing Resources of Columbia County

Using e-mail is inherently insecure. Confidential information, including account numbers, credit card numbers, etc., should never be transmitted via e-mail or e-mail attachment. NCLC is not responsible for the loss or unauthorized disclosure of confidential information sent to NCLC via e-mail or attachment. This e-mail message is confidential and/or privileged and is for the use of the intended recipient only. All other use is prohibited.

<Experian Oct 2015 Data Breach letter.pdf.secure>



**Barrett Burns** President & CEO [barrettburns@vantagescore.com](mailto:barrettburns@vantagescore.com)

October 27, 2017

The Honorable Jeb Hensarling  
Chairman  
Committee on Financial Services  
U.S. House of Representatives  
Washington, D.C. 20515

The Honorable Maxine Waters  
Ranking Member  
Committee on Financial Services  
U.S. House of Representatives  
Washington, D.C. 20515

Dear Chairman Hensarling and Ranking Member Waters:

In 2005 the three national credit reporting companies (Experian, Equifax and TransUnion), convinced that tens of millions of creditworthy borrowers were not able to obtain a credit score using traditional models, assembled a "model development team" comprised of industry-leading experts on credit data, credit risk modeling, and analytics. The team was charged with designing a more predictive and inclusive credit scoring model; a model that would score more people with more accuracy and more consistency across all three CRCs. Leveraging its decades of collective analytical skills and its extensive credit data experience, the team developed cutting-edge, patented and patent-pending techniques that were able to analyze extensive, anonymous consumer credit data which more accurately reflected current economic conditions.

Prior to unveiling the VantageScore consumer credit scoring model in 2006, the CRCs formed a limited liability company, VantageScore Solutions, LLC, and transferred the intellectual property rights of the new model to VantageScore Solutions, an independently managed firm. VantageScore Solutions (not the CRCs) maintains, revalidates, and updates the scoring model and educates lenders, consumers, and policymakers about its benefits.

Since its inception, VantageScore has developed additional versions of its generic credit scoring model, all of which continue to deploy a consistent algorithm across each of the three national credit reporting companies ("CRCs"). In choosing to work exclusively with credit file data, VantageScore has benefitted from the stringent regulations (i.e., ECOA and FCRA) and data standards (e.g., quality, accuracy, standardization, and universality) that such data are subject to. Our models are used variously in each part of the credit process. From the beginning, VantageScore has been committed to scoring as many consumer credit files as can be scored both responsibly and predictably.

Since its introduction in 2006, the VantageScore credit scoring model has experienced significant market acceptance. More than eight billion VantageScore credit scores were used in a 12-month period



in 2015–2016—an increase of nearly 40% over 2014–2015. Over 2,400 lenders and other industry participants—including 20 of the top 25 financial institutions—used VantageScore credit scores from July 2015–June 2016. Some of the most sophisticated secondary market participants also use the VantageScore model to help evaluate and monitor risk. In addition, the credit rating agencies have evaluated loans based on the VantageScore model.

VantageScore competes in the credit scoring marketplace with FICO. FICO's credit bureau risk scores were made available to the three national CRCs in 1991. In the intervening years since that introduction, both our nation's demographics and behaviors have changed tremendously, as have the credit files that document those behaviors: expanding in scope, reach, and granularity. Yet as late as the early 2000s, those credit files still didn't distinguish between student and retail installment loans, or between first and second mortgages. Newer models are built on the more granular data that has become available. The forthcoming model from VantageScore, Version 4.0, will be the first and only tri-bureau credit scoring model to use "trended" credit file data, which considers changes in consumers' behaviors over time.

In the intervening years, FICO has never once changed its minimum rules for who gets a generic score and who doesn't; a tradition driven by FICO's own commercial preferences. VantageScore, on the other hand, has demonstrated how millions of additional consumers – unscoreable using the FICO legacy models and dubbed "credit invisibles" by many, including the Consumer Financial Protection Bureau (CFPB) – can be scored using credit file data. A meaningful subset of that group demonstrates risk profiles that could potentially qualify them for prime or near-prime pricing on consumer loans.

In further contrast to FICO, VantageScore routinely analyzes and publishes the statistical validations of its models' predictive power in all populations. Those reports are freely downloadable on our public website (ex., <https://www.vantagescore.com/images/resources/VS3-2014Validation.pdf>). Thus, the ability to confirm VantageScore's claims of predictiveness is made available for all. Perhaps most importantly: when lenders implement VantageScore, they further test VantageScore's claims of predictiveness and inclusion, using their own data.

Clearly, both FICO and VantageScore think *their approach* is best. The beauty of competitive markets is that they let customers (lenders, insurers, landlords, utility companies, and other users of credit scores) decide for themselves. As a result of this competition, lenders now use VantageScore credit scores for many different purposes, including marketing, underwriting, pricing, portfolio management, model building, testing and validation.

Yet from the beginning, FICO has strongly resisted the possible introduction of competition in the credit scoring marketplace. To block VantageScore's entry into the market, FICO went to court in 2006, soon after VantageScore was formed, asserting, among others, claims against VantageScore for alleged violations of antitrust laws. In a noteworthy decision the District Court held that:

*"...Fair Isaac's antitrust claims suffer from a fundamental, indeed fatal, flaw. The alleged conspiracy does not employ tactics that seek to destroy or cut off competition before it even has a chance to take hold; rather, the alleged conspiracy is dependent on convincing the*



market...that greater value can be realized by switching from FICO scores to VantageScore credit scores. This is the very essence of competition." [emphasis added]

Since that time FICO has continued to take steps to quash competition. Its attacks on VantageScore are simply thinly-veiled and unsuccessful attempts to discredit its principal competitor.

The use of VantageScore credit scores has nonetheless surged, despite its effective exclusion from the mortgage sector since the first VantageScore model was introduced. This exclusion is the result of Fannie Mae and Freddie Mac's current seller-servicer guidelines, which require any mortgage lender that wishes to sell its loans to either Fannie or Freddie, via the GSEs' automated systems, to underwrite its loans using the FICO 04 model.<sup>1</sup> Many find it mind-boggling that the Federal Housing Finance Agency (FHFA), as the regulator and conservator of Fannie and Freddie, would allow that requirement to continue to stand since the requirement is not dictated by law or regulation, was not subject to a notice and comment requirement, and mandates the use of a pre-recession credit scoring model built using data from 1995 to 2000.

Yet the requirement nonetheless continues. As FICO CEO Will Lansing commented on February 27, 2013, when asked about competitors:

*"There are alternatives that credit bureaus themselves have developed a score called VantageScore. It has not gotten a lot of traction and all 3 bureaus still sell FICO Scores happily to the banks. So there's not that much competition around our Scores business. We have a – we're kind of designed in, in a lot of places ... For example, Fannie and Freddie have mandated that FICO Scores have to be part of a mortgage origination. So that puts you (i.e. FICO) in a very low risk territory. But even where it's not a matter of law, as a matter of practice, the Scores are really deeply embedded. So not a lot of risk there ..."*

There was a time when Fannie Mae and Freddie Mac's longstanding policy of requiring that loans be underwritten using the FICO 04 model made sense. It was a time when there were no other alternatives. However, perpetuating FICO's de facto monopoly despite the fact that there are newer credit scoring models readily available in the marketplace that are both more predictive and more inclusive simply because FICO is "*really deeply embedded*" redounds to the detriment of many American consumers.

VantageScore neither advocates now nor has it ever advocated the implementation of a policy that would **require** lenders to use VantageScore; but we are staunch advocates of a policy that would **allow** lenders to choose from among several **validated** scoring models (that is, models that meet the highest standards of performance based on analyses conducted by Fannie Mae, Freddie Mac, or any lender choosing to use them).

And we are not alone in that regard. Many others have voiced concern with the GSEs' insistence that lenders use a timeworn credit score rather than state-of-the-art competitive models. For example:

<sup>1</sup> Specifically, the Equifax Beacon 5.0, Experian/Fair Isaac Risk Model V25M, and TransUnion FICO Risk Score Classic 04 are mandated.



- The Mortgage Bankers Association (MBA) wrote to FHFA Director Mel Watt on November 5, 2014:

*"As the nation's housing markets continue their slow recovery, we are concerned that the GSEs' continued use of outdated credit scoring models may be adversely impacting the cost of credit for some American families—especially first-time, minority and moderate-income buyers."*

- Syndicated real estate columnist Ken Harney in a December 3, 2016, column under the headline ***When will Fannie and Freddie switch to a new credit-scoring model?*** (<http://newsok.com/article/5528899>) wrote:

*The two behemoths of the mortgage business, Fannie Mae and Freddie Mac, continue to use a credit scoring model that even its developer, FICO, says is not as "predictive" as its much newer models. Worse yet, Fannie and Freddie require that all lenders who want to submit loan applications to them must also use the same, outdated technology.*

- In testimony before your Committee on "Sustainable Housing Finance" on October 25, 2017, Richard Stafford (President & CEO of Tower Federal Credit Union), testifying on behalf of the National Association of Federally-Insured Credit Unions (NAFCU), addressed the issue of credit score competition at the GSEs in his written witness statement (p.16):

*"NAFCU would also like to caution Congress against perpetuating the use of just one brand of credit-scoring model. Both Fannie Mae and Freddie Mac require loans that are underwritten using FICO scoring models. A new housing finance system should be open to alternative credit scoring models as well. NAFCU supports legislation that would allow alternative credit scoring models to be used."*

- The Structured Finance Industry Group (SFIG) wrote to cosponsors of the "Credit Score Competition Act" (H.R. 898) on April 11, 2017:

*However, in the narrow context of whether any one particular credit score developer should be mandated by name in the GSEs' seller guides, SFIG sees no reason why that should be the case. We know of no other area in which the GSEs have mandated the exclusive use of a single supplier – compare, for example, the GSEs' approach to mortgage insurance with their current approach to credit score developers. It would seem to us that having the GSEs maintain a list of approved credit score models and allowing mortgage originators to choose among them (a choice that may involve obtaining more than one credit score) makes sense.*

As regulator and conservator of the GSEs, the Director of FHFA could open the GSEs' credit score requirements to include other more predictive and more inclusive scores, thus broadening access to mainstream pricing without lowering standards – something FHFA has been considering for many years. Such action would eliminate the scoring monopoly created by the GSEs and introduce the benefits of competition.





In addition, two of your colleagues on the House Financial Services Committee, Representative Ed Royce and Representative Kyrsten Sinema, have introduced the bipartisan "Credit Score Competition Act" (H.R. 898) which would require the GSEs to develop a process to evaluate other credit score models and make publicly available the process they will use to validate other credit scoring models for use in the underwriting of loans to be sold to the GSEs. The "Credit Score Competition Act" is cosponsored by 5 Republicans and 7 Democrats (including Representatives Royce and Sinema). It was one of a number of bills that were the subject of a hearing in the Financial Institutions and Consumer Credit Subcommittee on September 27, 2016. While the 1<sup>st</sup> Session of the 115<sup>th</sup> Congress will soon be ending, I would nevertheless urge you to bring this bill before both the Committee and the House if possible.

Thank you for your consideration of these issues. I would be pleased to meet to discuss the issues addressed in this letter with you and/or your staff at your convenience. To arrange a meeting or if you would like additional information please don't hesitate to contact me at [barrett.burns@vantagescore.com](mailto:barrett.burns@vantagescore.com) or (203) 363-2161, or our Washington counsel, Bill Donovan, at [wjdonovan@wjdonovanlaw.com](mailto:wjdonovan@wjdonovanlaw.com) or (703) 254-6633.

Sincerely,

A handwritten signature in cursive script that reads 'Barrett Burns'.

## The New York Times

FAIR GAME

### *Equifax's Grip on Mortgage Data Squeezes Smaller Rivals*

By Gretchen Morgenson

Oct. 13, 2017

Like it or not, when you apply for a home mortgage or to refinance an existing loan, Equifax will be a part of the process.

That's because, of the three major credit reporting agencies, only Equifax has a division, Equifax Mortgage Solutions, that supplies lenders with what is known as a merged credit report. These reports, which borrowers pay for, compile information provided by Equifax and the other two major credit reporting agencies, Experian and TransUnion.

As with much else about the credit-reporting industry, you don't have a choice about who provides your information. Mortgage lenders need to know your credit standing when they consider whether to give you a loan, and while other credit-reporting companies can provide a merged report, Equifax is a major go-to source for that information.

This is a very big business for Equifax. The mortgage solutions unit generated \$142 million in operating revenue last year, up 15 percent from 2015. The unit accounted for 11.5 percent of Equifax's operating revenue last year.

Given that the company's lapses recently allowed hackers to steal personal information belonging to as many as 145.5 million consumers, Equifax's dominance in this arena is unfortunate.

Even more troubling is a deal between Freddie Mac, the huge mortgage-finance company, and Equifax that gave the troubled credit reporting agency an even tighter grip on the business of providing credit information.

You have 3 free articles remaining.  
Subscribe to The Times

9/18/2018

Equifax's Grip on Mortgage Data Squeezes Smaller Rivals - The New York Times

Here's the background. Both Freddie Mac and the other government-sponsored mortgage finance company, Fannie Mae, have automated underwriting systems that are meant to make their loan guarantee or purchasing processes work smoothly and quickly. Mortgage lenders rely on them heavily.

A borrower's credit standing is a crucial piece of the information that flows into these systems. While Equifax and the other big credit-reporting agencies dominate, a group of about 40 other firms also provide lenders with credit information. In addition to supplying merged credit reports as Equifax does, these firms often provide more detailed information, including verification of a borrower's employment, and past payments to utilities, phone companies and landlords.

That these independent companies can still operate in a world that Equifax dominates may be an indication that they provide superior customer service such as quickly correcting errors or outdated information in a report. Equifax can supply the same information, but its customer service is not so stellar. The internet abounds with consumer complaints about the company, and since the data breach, many consumers have said they have been unable to reach the company.

That is what comes of having little or no competition. Which is why it is troubling that Freddie Mac has decided to allow Equifax to ban dozens of rival credit-reporting companies from one part of its automated system.

Freddie Mac recently developed Loan Quality Advisor, a new part of that system. It was, according to the company's website, a "risk and eligibility assessment tool that evaluates loan data to help lenders determine if a loan is eligible for sale to Freddie Mac."

Naturally, a borrower's credit history goes into this system. But Freddie Mac assigned gatekeeper status to Equifax, essentially allowing it to bar an array of competing firms from providing credit information during the process.

This change hurts competitors by ensuring that what could be their business goes to Equifax instead. But it may also harm certain borrowers. Because of the more efficient services the other firms often provide, preventing them from participating could make it more difficult for borrowers with errors on their credit histories to correct them in time to secure a mortgage.

(Fannie Mae has taken a different approach with its automated loan-underwriting system. Its structure is more open, allowing independent credit-information providers to participate at multiple levels)

Interestingly, an internal Freddie Mac email indicates that Equifax drove the decision to keep independent companies, known as technical affiliates, out of the system.

9/18/2018

Equifax's Grip on Mortgage Data Squeezes Smaller Rivals - The New York Times

"Equifax chose not to make adjustments to be able to accommodate the T.A.s," wrote an official in Freddie Mac's Vendor Technology Integration unit. Because Equifax "chose not to add functionality to support," she added, "we were unable to support as a result."

I asked Equifax why it was keeping so many competitors, most of them smaller, off the Freddie Mac system. Wyatt Jefferies, a spokesman, did not respond directly, saying only that Equifax "operated within existing Fair Credit Reporting Act guidelines" with all the independent companies.

In light of the recent data breach at Equifax and deep consumer unease about the company's practices, I thought Freddie Mac might be rethinking its granting Equifax what amounts to most favored nation status.

It is not. Chad Wandler, a Freddie Mac spokesman, said that having access to a broad network of credit-report providers "has not been cited as a priority for those customers who use our quality control tools like Loan Quality Advisor." He added, "We will continue to listen to our customers to provide the functionality they need."

Naturally, this does not sit well with independent credit-reporting companies.

"What we're talking about here is to provide the consumer with a touch point of service that is different than what you get from the bureaus," said Terry Clemans, executive director of the National Consumer Reporting Association, an organization of credit-reporting agencies, employment-screening services and tenant-screening companies. "But Equifax has elected to not let these companies compete, and Freddie Mac has put them in that position to allow it."

Given that Freddie Mac is owned by taxpayers, lawmakers may be interested in its dealings with Equifax. In the past week, Senator Sherrod Brown, Democrat of Ohio, asked the Treasury Department to prohibit Equifax from eligibility for government contracts, saying the company did not deserve to earn taxpayer money. (On Thursday, the Internal Revenue Service, a unit of the Treasury, said it had suspended a \$7.2 million contract it awarded to Equifax last month.)

Amid all this, it is noteworthy that Equifax imposes higher costs than competitors for some of its credit-reporting services. In an Equifax email in September 2016 about a price increase at the company, an employee said that it charged its competitors, who must buy the information, two to three times the combined costs charged by Experian and TransUnion.

Mr. Jefferies, the Equifax spokesman, declined to comment on the agency's pricing. But he said in a statement that the company's price adjustments "reflect investments we are making to ensure we are delivering market-leading innovation and technology to customers."

9/18/2018

Equifax's Grip on Mortgage Data Squeezes Smaller Rivals - The New York Times

Unlike its competitors, Equifax also charges more for a type of credit report used by housing counselors who work with troubled consumers to get their finances back on track.

There are two types of credit reports — a “hard pull” and a “soft pull.” A hard pull is requested by a lender looking to extend credit to a consumer. A soft pull, by contrast, is used by loan counselors to get a fix on a consumer’s credit standing.

Most credit-reporting companies charge the same for both types of reports. Not Equifax. It charges twice as much for a soft pull as it does for a hard pull, housing counselors said.

“The role of housing counseling and assisting people getting and maintaining credit is really crucial,” said Bruce Dorpalen, executive director of the National Housing Resource Center in Philadelphia, an advocacy organization for nonprofit housing counselors. “To penalize them by charging extra for a credit report is disadvantaging people when they need help the most.”

Mr. Jefferies of Equifax declined to comment on this practice.

Let’s have a show of hands out there. How many think Equifax should have even more control and sway in the credit reporting industry than it already has?

Noted.

Twitter: @gmorgenson

A version of this article appears in print on Oct. 15, 2017, on Page BU1 of the New York edition with the headline: Equifax Grip Puts Squeeze On Its Rivals

**Questions for Mr. Richard F. Smith, Former Chairman and Chief Executive Officer of Equifax, Inc. from Ranking Member Maxine Waters**

In your testimony you wrote that throughout your tenure as CEO of Equifax, your firm took data security and privacy extremely seriously, and that your company devoted substantial resources to it.

**Waters Question #1:** If this is the case, how is it possible that upon learning from the U.S. Department of Homeland Security's Computer Emergency Readiness Team of a key vulnerability in versions of software used by Equifax, your security team did not take any action in a timely manner? Doesn't the fact that no immediate action was taken upon being notified about a potential vulnerability by the Department of Homeland Security, suggest that your company didn't in fact take these issues that seriously?

A: As set forth below, the Equifax security team took immediate action upon being notified of a potential vulnerability. The breach occurred because of both human error and technology failures, not because Equifax failed to take these issues seriously.

On March 9, 2017, Equifax disseminated the U.S. Department of Homeland Security, Computer Emergency Readiness Team ("U.S. CERT") notification internally by email requesting that personnel responsible for an Apache Struts installation immediately upgrade their software. Consistent with Equifax's patching policy, the Equifax security department required that patching occur within a 48 hour time period. Equifax now knows that the vulnerable version of Apache Struts existed within Equifax but was not identified or patched in response to the internal March 9 notification to information technology personnel.

On March 15, 2017, Equifax's information security department also ran scans that should have identified any systems that were vulnerable to the Apache Struts issue identified by U.S. CERT. The scans, however, did not identify the Apache

Struts vulnerability. Unfortunately, Equifax's efforts undertaken in March 2017 did not identify any versions of Apache Struts that were subject to this vulnerability.

That said, Equifax has implemented several updates to protocols and procedures in response to this incident. Vulnerability scanning and patch management processes and procedures have been enhanced. The scope of sensitive data retained in backend databases has been reduced so as to minimize the risk of loss. Restrictions and controls for accessing data housed within critical databases have been strengthened. Network segmentation has been increased to restrict access from internet facing systems to backend databases and data stores. Additional web application firewalls have been deployed, and tuning signatures designed to block attacks have been added. Deployment of file integrity monitoring technologies on application and web servers has been accelerated. The Company is also implementing additional network, application, database, and system-level logging. These are just a few of the steps Equifax has taken since the breach was discovered to shore up its security protocols.

Equifax's forensic consultants have recommended and are implementing a series of improvements that are being installed over 30, 60, and 90 day periods. Equifax also engaged PwC to assist with its security program, including strategic remediation and transformation initiatives that will help Equifax identify and implement solutions to strengthen its long-term data protection and cyber security posture.

Beyond the technological enhancements, Equifax has also made several strategic personnel changes at the highest levels of the company since September 7, 2017. The CEO stepped down and the Chief Information Officer and Chief Security Officer also resigned from their positions.

**Waters Question #2: In another example that underscores the low value your company placed on protecting consumers' data, researchers at a Wisconsin-based company called Hold Security discovered that an Equifax web portal was secured by the default username and password combination "admin and admin." Can you comment on how this type of easily-exploited password vulnerability was accepted at Equifax?**

A: The use of such passwords was against Equifax policies. Further, Equifax has implemented several updates to protocols and procedures in response to this incident. Vulnerability scanning and patch management processes and procedures have been enhanced. The scope of sensitive data retained in backend databases has been reduced so as to minimize the risk of loss. Restrictions and controls for accessing data housed within critical databases have been strengthened. Network segmentation has been increased to restrict access from internet facing systems to backend databases and data stores. Additional web application firewalls have been deployed, and tuning signatures designed to block attacks have been added. Deployment of file integrity monitoring technologies

on application and web servers has been accelerated. The Company is also implementing additional network, application, database, and system-level logging. These are just a few of the steps Equifax has taken since the breach was discovered to shore up its security protocols.

Equifax's forensic consultants have recommended and are implementing a series of improvements that are being installed over 30, 60, and 90 day periods. Equifax also engaged PwC to assist with its security program, including strategic remediation and transformation initiatives that will help Equifax identify and implement solutions to strengthen its long-term data protection and cyber security posture.

Equifax has also implemented certain technological remediation steps as described in the Mandiant executive summary, which was submitted to this Committee on October 1, 2017.

**Waters Question #3: Your testimony notes that in addition to obtaining dispute documents from Equifax's online web portal, hackers "may have accessed a database table containing a large amount of consumers personally identifiable information (PII), and potential other data tables." Can you comment on why Equifax would ever find it necessary to store large amounts of consumers' sensitive personal information in a table that hackers could easily exploit?**

A: Please see response to Waters Question #2.

**Waters Question #4: I understand that on July 29th Equifax's security team identified "suspicious network traffic" as part of its online dispute portal. Is that correct? How do Equifax's internal documents or manuals providing guidance to its employees in this area define the term "suspicious" traffic? Does suspicious traffic suggest in any way that sensitive customer information may have been compromised?**

A: On July 29, 2017, Equifax's security team observed suspicious network traffic associated with the U.S. consumer online dispute portal web application where consumers can upload documents or other information in support of a credit file dispute. In response, the security team investigated and immediately blocked the suspicious traffic that was identified. The security team continued to monitor network traffic and observed additional suspicious activity on July 30, 2017. In response, they took the web application completely offline that day. At that time, the security team did not recognize that any sensitive consumer PII had been compromised. The hard work to figure out the nature, scope, and impact of the hack then began, including whether personal identifying information ("PII") had been stolen. The term "suspicious traffic" is not defined in Equifax's relevant internal guidance documents.

Mandiant, a leading independent cybersecurity firm, was engaged to investigate this incident. Mandiant has provided Equifax with an executive summary, a supplemental



report, and a final supplement. Equifax has provided these documents to the Committee previously.

**Waters Questions #5.3 and #5.4:** Does your internal legal department, or chief legal officer, have specified circumstances or even guidance in which that person is given authority to retain outside legal counsel relating to or because of a breach or unauthorized exposure of data? Does the cybersecurity team, or the chief information or security officer, have specific circumstances, or even guidance, in which that division or executive is authorized to retain an outside cybersecurity company?

A: As of May 2017, Equifax had in place several plans to address cybersecurity incidents and various types of crises. Among other topics, those plans contemplate retaining outside legal counsel and/or outside cybersecurity companies in connection with responding to a cybersecurity incident. For additional details regarding the plans and protocols in place to address a cybersecurity incident, please see the response to the question from Rep. Meeks provided below.

**Waters Questions #7.1 and #7.2:** Despite the sensitivity of the information that was compromised as part of the Equifax breach, which included names, Social Security Numbers, birth dates, addresses, and even driver's license numbers, and credit card information in some cases, Equifax did not opt to directly notify each of the affected individuals. Instead, Equifax has placed this burden on American consumers. Mr. Smith, do I have this right? Your current policy is that it is the victims' responsibility to determine whether they have been harmed, not the responsibility of the company that allowed their information to be stolen. Can you discuss how Equifax determined that it didn't need to notify affected consumers?

A: Equifax has notified consumers potentially impacted by this incident consistent with data breach notification laws. On September 7, 2017, Equifax provided notification of the incident by issuing a nationwide press release, providing a dedicated website where consumers could determine if they were impacted and sign up for a free credit file monitoring and identity theft protection product, and by providing a dedicated call center for consumers to obtain more information. The notification indicated that the incident impacted personal information relating to approximately 143 million U.S. consumers, primarily including names, Social Security numbers, birth dates, addresses and, in some instances, driver's license numbers.

Equifax also mailed written notices to consumers whose credit card numbers or dispute documents were impacted as well as to the approximately 2.5 million additional potentially impacted U.S. consumers identified since the September 7 announcement and notification.

In addition to Equifax's commitment to notify potentially affected consumers, Equifax provided notification pursuant to data breach notification statutes that impose various notice requirements for consumers. Equifax's notification included both substitute

notification contemplated by the data breach statutes using a nationwide press release, dedicated website, and call center, and through direct mail notification for certain groups of potentially impacted consumers.

**Waters Question #8:** In your written testimony, you wrote that “we at Equifax clearly understood that the collection of American consumer information and data carries with it enormous responsibility to protect that data.” And you go on to say that you “apologize to the American people.” Mr. Smith, I’m sure the American people can appreciate that you are sorry, and I’m glad to hear that you understand that your firm is responsible for this compliance failure, but in addition to being “sorry” I’d like to know, who at your firm is actually being held accountable. To the extent that any executives who were directly responsible for addressing the vulnerability that had been identified by the Department of Homeland Security failed to do so, what specific changes has Equifax implemented to prevent this from occurring again?

A: At the time the breach was discovered, David Webb was Equifax’s Chief Information Officer, Susan Mauldin was Equifax’s Chief Security Officer, and Richard Smith was Equifax’s CEO. The individual who oversaw the team responsible for patching the relevant Apache Struts vulnerability on software supporting Equifax’s online disputes portal reported to Mr. Webb. Both Mr. Webb and Ms. Mauldin resigned from their positions, effective September 15, 2017 and Mr. Smith stepped down as CEO on September 25, 2017.

**I would appreciate it if you could respond to my series of questions with a simple yes or no, given the short question and answer time period:**

**Waters Question #9.1:** Is the current estimation from your company that 145.5 million American consumers have had their personally identifiable information and sensitive financial information, exposed to bad actors?

A: Yes, we currently estimate that 145.5 million consumers’ personal information was impacted. We believe that the best way for consumers to protect themselves and prevent any harm from occurring as a result of the incident is to enroll in TrustedID Premier and utilize the free lock service, which Equifax will offer at the end of January.

**Waters Question #9.2:** Have your previous statements indicated that the company’s dispute complaint portal was the sole entry point in which consumers’ data was exposed?

A: Yes.

**Waters Question #9.3:** Does the fact that 145.5 million consumers’ data was exposed indicate that 145.5 million consumer complaints were submitted to Equifax?

A: No.

**Waters Question #9.4:** Let's end this confusion right now, did the firm's dispute complaint portal act as an open door that allowed bad actors to come into Equifax database in other areas that then resulted in the exposure of consumers' data outside of the dispute complaint portal because, otherwise, I'm confused about how the number of consumers has been determined?

A: Mandiant, a leading independent cybersecurity firm, provided Equifax with an executive summary, a supplemental report, and a final supplement, which collectively detail Mandiant's and Equifax's review process for determining the scope of data exposure for U.S. consumers. Equifax has provided these documents to the Committee previously.

**Waters Question #18:** On October 5, 2017, you testified that Equifax maintained a process for clearing the sale of Equifax securities by the company's officers. Please provide a detailed description of this process as it existed in August 2017. Did Equifax maintain a written policy reflecting this process? If so, please attach any and all documents in your possession evidencing a written policy. How did Equifax ensure that all relevant employees were aware of and adhered to this process? In your view, did these processes adequately prevent Equifax employees from trading Equifax securities in the days between insider awareness and public disclosure of a materially significant event?

A: The Board of Directors of Equifax released a report by the Special Committee of the Board of Directors on November 1, 2017, regarding the trading of Company securities by certain executives following the detection by Equifax cybersecurity personnel of suspicious activity in the Company's network and prior to public disclosure of the incident. A copy of the report by the Special Committee is enclosed. In addition, a copy of the Insider Trading Policy is provided with this submission at Bates numbers EFXCONG-HFSC000000001-EFXCONG-HFSC000000014.

Equifax provides notification to all employees subject to pre-clearance requirements that a trading window is about to open and reminding these employees that they are subject to the company's insider trading policy and are required to pre-clear all transactions. The notification provided on July, 25, 2017 is provided with this submission at Bates numbers EFXCONG-HFSC000000015-EFXCONG-HFSC000000016. Equifax also provides a similar notification (absent reference to the pre-clearance requirement) to all employees that are permitted to trade only during the trading window.

**Waters Question #24:** Given that Equifax just lost the personally identifiable information for half of the U.S. adult population, I was surprised to learn that the Trump Administration just last week approved a contract for Equifax to "verify taxpayer identity" and "assist in ongoing identity verification and validations" on behalf of the IRS.

**Given Equifax's clear inability to safeguard consumers' data, will you agree to reject this and enable the IRS to designate a different company for this contract?**

A: On September 29, 2017, Equifax was awarded a bridge contract (task order number TIRNO-17-K-00497 issued against contract number GS00F159DA) to continue providing identification verification and validation services to the IRS while GAO was considering Equifax's protest of the IRS's award of a longer-term contract to provide those services. On October 12, 2017, Equifax received written notice from the IRS to stop work under the subject contract. On October 16, 2017, GAO denied Equifax's bid protest.

**Questions for Mr. Richard F. Smith, Former Chairman and Chief Executive Officer of Equifax, Inc. from Rep. Keith Ellison**

**Ellison Question #9.1:** It is my understanding that the short-term \$7.25 million contract awarded to Equifax was a bridge contract because of a contract dispute your former firm had with the IRS. The IRS wanted to bid the contract out to other vendors and Equifax disputed this change. So the bridge contract was to prevent a lapse in service during a protest on another contract. Is that information correct?

A: Please see response to Waters Question #24.

**Ellison Question #9.2:** On what basis did Equifax protest the IRS's action to rebid the contract?

A: Equifax's bid protest, which was filed on July 7, 2017, in accordance with 4 C.F.R. § 21.2(a)(2), enumerates Equifax's grounds for submitting the protest to GAO. Equifax protested because it believed IRS's evaluation was inconsistent with the terms of the solicitation. The basis of protest was two-fold. First, Equifax did not believe that Experian could meet the connection requirements described in the solicitation. Second, it appeared that Experian proposed to provide IRS with services that were materially different from the services required by the Solicitation. The protest alleged that IRS's evaluation, which found Experian technically acceptable notwithstanding these issues, was not conducted in accordance with the stated evaluation criteria. On October 16, 2017, GAO denied the bid protest.

**Ellison Question #15:** Was Equifax's market capitalization rate \$13.2 billion? If not, what was it?

A: In Equifax's most recent Form 10-Q securities filing, filed on November 9, 2017, the Company reported that it had approximately 120 million shares of common stock outstanding as of September 30, 2017. On October 2, 2017, which was the next day markets were open, Equifax's stock closed at \$107.81. Based on those values, Equifax had a market capitalization of approximately \$12.9 billion when the markets closed on October 2.

**Ellison Question #16:** Did Equifax earn \$3.1 billion of revenue last year? If not, how much in revenue did Equifax earn?

A: Equifax reported \$3.1 billion of operating revenue for twelve months ending on December 31, 2016 in its Form 10-K securities filing, filed on February 22, 2017.

**Ellison Questions #17.1 and #17.2:** Does Equifax have 9,500 employees? If not, how many employees does Equifax have?

A: As of December 1, 2017, Equifax has approximately 10,000 employees.

**Questions for Mr. Richard F. Smith, Former Chairman and Chief Executive Officer of Equifax, Inc. from Rep. Denny Heck**

**Heck Question #1: When did Equifax first notify the Federal Bureau of Investigation about the breach?**

A: Equifax notified the Federal Bureau of Investigation about the incident in question on August 2, 2017.

**Heck Question #2: When did Equifax first notify a state law enforcement agency about the breach?**

A: Equifax provided written notifications to 52 state attorneys general on September 7, 2017. Upon the completion of the forensic investigation, Equifax also provided supplemental notifications to those 52 state attorneys general on October 12, 2017.

**Heck Question #3: When did Equifax first notify the Federal Trade Commission about the breach?**

A: Equifax notified the Federal Trade Commission about the incident in question on September 7, 2017.

**Heck Question #4: When did Equifax first notify the Consumer Financial Protection Bureau about the breach?**

A: Equifax notified the Consumer Financial Protection Bureau about the incident in question on September 7, 2017.

**Heck Question #6: Will Equifax take any steps to reach out to all approximately 145 million people whose information was stolen in the hack? If not, how does it decide which people to attempt to directly notify and which to rely on media and people coming to the Equifax website?**

A: Please see the response to Waters Questions #7.1 and #7.2.

**Heck Question #10: Is Equifax taking any actions proactively to protect individuals whose information was stolen in the breach?**

A: Equifax has taken a number of steps to notify and help protect individuals whose information was potentially impacted, including the following:

- Equifax created a website ([www.equifaxsecurity2017.com](http://www.equifaxsecurity2017.com)) to notify and inform consumers about the incident. The website includes: (1) information about the incident; (2) a tool for consumers to learn if they were impacted; (3) identity theft

prevention tips; and (4) information about Equifax's free TrustedID Premier product.

- Equifax set up dedicated call centers to assist consumers affected by the incident. Since the incident was announced, Equifax has scaled up these operations to ensure it has more than enough associates to handle calls from concerned consumers.
- Until January 31, 2018, consumers can enroll in a free one-year product called TrustedID Premier, which includes:
  - Free credit monitoring with all three consumer credit bureaus;
  - Free access to Equifax credit reports for one year;
  - Free scanning of Social Security numbers against suspicious websites;
  - A free credit report lock feature; and
  - Identity theft insurance of up to \$1 million.
- By January 31, 2018, Equifax will offer a new service that will allow consumers to lock and unlock their Equifax credit file, for free, for life.

**Heck Question #14: How has Equifax changed its process for patching vulnerabilities since discovering the breach?**

A: Since discovering the breach, Equifax has improved its patching procedures to require a "closed loop" confirmation that necessary patches have been applied, rolled out a new scanner to identify vulnerabilities, upgraded its security technology, and increased accountability mechanisms for Equifax Security team members.

**Heck Question #18: Equifax has stated that it identified records affected by reconstructing the queries used to access the database. What characteristics was the hacker searching for?**

A: Mandiant, a leading independent cybersecurity firm, was engaged to investigate this incident. Mandiant has provided Equifax with an executive summary, a supplemental report, and a final supplement. Equifax has provided copies of these documents to the Committee previously.

**Heck Question #23: Does Equifax have written procedures laid out for notifying executives about a security breach?**

A: As of May 2017, the company had in place several plans to address cybersecurity incidents and various types of crises, which include but are not limited to the following:

- A Security Incident Handling Policy & Procedures document, which dates back to 2008, and a Security and Safety Crisis Action Plan document, which dates back to 2013. These guides and plans were in place in May 2017 and have been updated and refined over time, including changes to the titles of the operative documents.
- A Crisis Management Plan (“CMP”), Parts I and II that has been in place dating back to 2013. The CMP plan covers a variety of crises, including data breaches.
- A Crisis Action Team (“CAT”) Plan specific to certain geographic regions within the Company. The CAT plan, like the CMP described above, covers a variety of crises, including data breaches.

Equifax faces numerous cyber threats every day. Its Cyber Threat Center (“CTC”) constantly assesses whether a particular threat can be resolved quickly by the Company’s own internal cybersecurity team, or whether the threat will require additional resources to remediate. If the CTC determines that a cybersecurity threat is unusual and will require additional resources to contain, it is typically designated a “Security Incident” and Equifax’s response outlined in the Security Incident Handling Policy & Procedures is triggered.

As set forth in the Security Incident Handling Policy & Procedures, once a Security Incident has been declared, its severity is classified based on a risk assessment including:

- number of affected systems;
- network impact;
- business services impact;
- sensitivity of information threatened or compromised; and
- the potential for harm.

Various senior officers, including those within the Legal Department, are notified by security of Security Incidents and typically outside experts are retained (e.g., a forensic team and outside counsel) to assist with the response.

**Heck Questions #25 and #26: On what date was Chief Legal Officer John Kelley made aware of the breach? On what date did Chief Legal Officer approve the early August stock sales by other Equifax executives?**



A: On July 30, 2017, Chief Legal Officer John Kelley was made aware of the fact that unusual activity had been detected on Equifax's network the prior evening, but neither he nor anyone else at the Company was made aware of the scope of the intrusion until mid-August when Mandiant and the Equifax security department began to determine the level of unauthorized activity. The Board of Directors of Equifax released a report by a Special Committee of the Board of Directors on November 1, 2017, regarding the trading of Company securities by certain executives following the detection by Equifax cybersecurity personnel of suspicious activity in the Company's network and prior to public disclosure of the incident. A copy of the report by the Special Committee and accompanying press release was provided to the Committee on November 3, 2017. A copy of that report is also enclosed with this submission. The report concludes, among other things, that that preclearance for the four trades was appropriately obtained and that each of the four trades at issue comported with Company policy.

**Questions for Mr. Richard F. Smith, Former Chairman and Chief Executive Officer of Equifax, Inc. from Rep. Gregory Meeks**

During the House Committee on Financial Services (“the Committee”) hearing on October 5, 2017, Mr. Rick Smith testified that: Equifax had written documentation on crisis management; Equifax would provide the Committee with crisis management documentation; and Equifax had tested it. By letter dated October 12, 2017, Representative Meeks requested from Equifax documentation of its written plan on how to respond to a breach and the dates when that plan was tested.

Following up on Mr. Smith’s testimony and in response to the letter from Representative Meeks, Equifax confirms that as of May 2017 the company had in place, and had tested, several plans to address cybersecurity incidents and various types of crises, which include but are not limited to the following:

- A Security Incident Handling Policy & Procedures document, which dates back to 2008, and a Security and Safety Crisis Action Plan document, which dates back to 2013. These guides and plans were in place in May 2017 and have been updated and refined over time, including changes to the titles of the operative documents. In June 2017, prior to Equifax’s detection of suspicious activity related to the cybersecurity incident, the company conducted a table-top test exercise of the “Security Incident Handling Policy & Procedures.” That test focused on the company’s Cyber Threat Center managing a newly announced Microsoft vulnerability.
- A Crisis Management Plan (CMP), Parts I and II that has been in place dating back to 2013. The CMP plan covers a variety of crises, including data breaches. A table-top test exercise of this plan was performed in June 2016, including a scenario that involved data security incident components.
- A Crisis Action Team (CAT) Plan specific to certain geographic regions within the Company. The CAT plan, like the CMP described above, covers a variety of crises, including data breaches. Table-top tests are also conducted for these plans, including scenarios involving data security incident components. The Southeast Crisis Action Team plan, for example, was activated in March 2017 in order to run an actual test of the plan.

Equifax is submitting examples of the crisis management documentation in place in May 2017 to the Committee (updates have been made to these plans since that time), Bates numbered EFXCONG-HFSC000000017–EFXCONG-HFSC000000187.

Questions for Mr. Richard F. Smith, Former Chairman and Chief Executive Officer of  
Equifax, Inc. from Rep. Kyrsten Sinema

Sinema Question #3: What changes has Equifax made to the IT department that failed to address the Apache Struts vulnerability? In addition to detailing any staff that were fired as a result, please provide a list of changes to company best practices to ensure that software patches are installed in the prescribed timeframe.

A: Please see response to Waters Questions #1, #2, and #8.

\* \* \*



## CFPB Oversight Uncovers And Corrects Credit Reporting Problems

Bureau Report Outlines Accuracy and Other Issues That Bureau Supervision Has Taken Action to Address

MAR 02, 2017

**WASHINGTON, D.C.** — Today the Consumer Financial Protection Bureau (CFPB) released a report detailing the problems in the credit reporting industry that the Bureau has uncovered and corrected through its oversight work. Since launching its supervision of the credit reporting market, the CFPB has identified significant issues with the quality of the credit information being provided by furnishers and maintained by credit reporting companies. Today's report outlines the actions that the CFPB has taken to address these ongoing problems such as fixing data accuracy at credit reporting companies, repairing the broken dispute process, and cleaning up information being reported.

"Since we began our oversight work, the CFPB has been uncovering and correcting problems in the consumer reporting industry," said CFPB Director Richard Cordray. "Because of our work, important improvements are being made. Much more work needs to be done but our corrective actions are leading to positive changes that are benefiting consumers all over the country."

Consumer reporting companies are businesses that track information about a consumer, including credit history, deposit account history, and other consumer transactions. Such companies, which include what are popularly called credit bureaus or credit reporting companies or agencies, play a key role in the consumer financial services marketplace and in the financial lives of consumers. For example, the reports sold by the three largest consumer reporting companies – Equifax, Experian, and TransUnion – are used in determining everything from consumer eligibility for credit to the rates consumers pay for credit. The consumer reporting companies receive their information from furnishers, including both banks and nonbanks. Inaccurate information can lead to inaccurate reports and consumer and market harm.

Consumers continue to complain about the credit reporting industry in high numbers. The Bureau has handled approximately 185,700 credit reporting complaints as of Feb. 1, 2017. Consumers have said that when they dispute an item on their report, nothing changes even though federal law requires the consumer reporting company to conduct a reasonable reinvestigation and update the file to reflect any necessary changes or delete the item.

Consumers also frequently complain of debts already paid showing up on their report as unpaid and information that is not theirs being included in their report negatively affecting their credit scores.

In 2012, the CFPB became the first federal agency to supervise all sides of the credit reporting market, which includes the consumer reporting companies and providers of consumer financial products or services, many of whom furnish or use consumer reports. In 2013, the CFPB published a bulletin warning that the agency would hold furnishers accountable for their legal obligation to investigate consumer disputes forwarded by the consumer reporting companies. The bulletin also reminded companies that they must review all relevant information provided with the disputes, including documents submitted by consumers. The CFPB has also made efforts, including in a [consumer advisory](#), to educate the public about the importance of checking their credit reports, what to look for in their reports, and how to dispute mistakes. As outlined in today's special edition of Supervision Highlights, because of these widespread issues, CFPB supervision has aimed its work at:

- **Fixing data accuracy at consumer reporting companies:** Early on, examiners found that one or more of the consumer reporting companies lacked good quality control to check the accuracy of their consumer records. The CFPB directed them to make necessary changes, and they did. In recent exams, examiners have found that quality control programs have been instituted that include tests to identify whether reports are produced for the wrong consumer and whether reports contain mixed-up files. The companies are also taking better corrective actions when mistakes are identified, and making system improvements to prevent the same mistakes from happening again.
- **Repairing broken dispute processes at consumer reporting companies:** CFPB examiners discovered that one or more consumer reporting companies were not following federal requirements that said they must send a notice with the results of disputes to consumers. They also found one or more consumer reporting companies failing to consider documentation provided by the consumer on a disputed item. The CFPB directed these companies to improve their dispute investigation systems. Now, continued monitoring has shown that the consumer reporting companies have improved processes for investigating disputes and are improving response letters to consumers.
- **Cleaning up information from furnishers:** Through earlier reviews at banks and nonbanks, CFPB examiners found widespread problems with furnishers supplying incorrect information to the consumer reporting companies. The CFPB directed them to take steps to address these problems, such as maintaining evidence that they are accurately handling disputes and conducting reasonable investigations. Since then, several furnishers have dedicated more resources to ensuring the integrity of the information. This effort includes better investigations and handling of disputes, notifying consumers of results, and taking corrective action when inaccurate information has been supplied. Importantly, though, examiners continue to find numerous violations at one or more furnishers, particularly around deposit account information.

9/18/2018

CFPB Oversight Uncovers And Corrects Credit Reporting Problems | Consumer Financial Protection Bureau

The CFPB's approach when examining the credit reporting activities of supervised entities is just like its approach to examining other activities of supervised entities. Supervision includes a review of compliance systems and procedures, on-site examinations, discussions with relevant personnel, and requirements to produce relevant reports. The Fair Credit Reporting Act governs how companies handle consumers' information. When examiners find violations of law, they direct the companies to change their conduct and remediate consumers. When appropriate, the CFPB's supervisory activity also results in enforcement actions, such as the action against the furnisher Wells Fargo Bank for failing to update or correct inaccurate, negative information reported to credit reporting companies about student loans.

**Today's edition of Supervisory Highlights Credit Reporting Special Edition is available at:**  
**[http://files.consumerfinance.gov/f/documents/201703\\_cfpb\\_Supervisory-Highlights-Consumer-Reporting-Special-Edition.pdf](http://files.consumerfinance.gov/f/documents/201703_cfpb_Supervisory-Highlights-Consumer-Reporting-Special-Edition.pdf)** 

###

*The Consumer Financial Protection Bureau is a 21st century agency that helps consumer finance markets work by making rules more effective, by consistently and fairly enforcing those rules, and by empowering consumers to take more control over their economic lives. For more information, visit [www.consumerfinance.gov](http://www.consumerfinance.gov)*

**Prepared Testimony of Richard F. Smith  
before the U.S. House Financial Services Committee**

**October 5, 2017**

Chairman Hensarling, Ranking Member Waters, and Honorable Members of the Committee, thank you for the opportunity to testify today.

**Preliminary Statement**

I am here today to recount for this body and the American people, as best I am able, what happened when Equifax was hacked by a yet unknown entity and sensitive information of over 140 million Americans was stolen from its servers, and to outline the remediation steps the company took. We at Equifax clearly understood that the collection of American consumer information and data carries with it enormous responsibility to protect that data. We did not live up to that responsibility, and I am here today to apologize to the American people myself and on behalf of the Board, the management team, and the company's employees.

Let me say clearly: As CEO I was ultimately responsible for what happened on my watch. Equifax was entrusted with Americans' private data and we let them down. To each and every person affected by this breach, I am deeply sorry that this occurred. Whether your personal identifying information was compromised, or you have had to deal with the uncertainty of determining whether or not your personal data may have been compromised, I sincerely apologize. The company failed to prevent sensitive information from falling into the hands of wrongdoers. The people affected by this are not numbers in a database. They are my friends, my family, members of my church, the members of my community, my neighbors. This breach has impacted all of them. It has impacted all of us.

I was honored to serve as the Chairman and Chief Executive Officer of Equifax for the last 12 years, until I stepped down on September 25. I will always be grateful for the opportunity to have led the company and its 10,000 employees. Equifax was founded 118 years ago and now serves as one of the largest sources of consumer and commercial information in the world. That information helps people make business and personal financial decisions in a more timely and accurate way. Behind the scenes, we help millions of Americans access credit, whether to buy a house or a car, pay for college, or start a small business. During my time at Equifax, working together with our employees, customers, and others, we saw the company grow from approximately 4,000 employees to almost 10,000. Some of my proudest accomplishments are the efforts we undertook to build credit models that allowed and continue to allow many unbanked Americans outside the financial mainstream to access credit in ways they previously could not have. Throughout my tenure as CEO of Equifax, we took data security and privacy extremely seriously, and we devoted substantial resources to it.

We now know that criminals executed a major cyberattack on Equifax, hacked into our data, and were able to access information for over 140 million American consumers. The information accessed includes names, Social Security numbers, birth dates, addresses, and in

some instances, driver's license numbers; credit card information for approximately 209,000 consumers was also stolen, as well as certain dispute documents with personally identifying information for approximately 182,000 consumers.

Americans want to know how this happened and I am hopeful my testimony will help in that regard. As I will explain in greater detail below, the investigation continues, but it appears that the breach occurred because of both human error and technology failures. These mistakes – made in the same chain of security systems designed with redundancies – allowed criminals to access over 140 million Americans' data.

Upon learning of suspicious activity, I and many others at Equifax worked with outside experts to understand what had occurred and do everything possible to make this right. Ultimately we realized we had been the victim of a massive theft, and we set out to notify American consumers, protect against increased attacks, and remediate and protect against harm to consumers. We developed a robust package of remedial protections for each and every American consumer – not just those affected by the breach – to protect their credit information. The relief package includes: (1) monitoring of consumer credit files across all three bureaus, (2) access to Equifax credit files, (3) the ability to lock the Equifax credit file, (4) an insurance policy to cover out-of-pocket costs associated with identity theft; and (5) dark web scans for consumers' social security numbers. All five of these services are free and without cost to all Americans. Equifax also recently announced an important new tool that has been under development for months that will allow consumers to lock and unlock their credit files repeatedly, for life, at no cost. This puts the control of consumers' credit information where it belongs – with the consumer. We have also taken steps to better protect consumer data moving forward.

We were disappointed with the rollout of our website and call centers, which in many cases added to the frustration of American consumers. The scale of this hack was enormous and we struggled with the initial effort to meet the challenges that effective remediation posed. The company dramatically increased the number of customer service representatives at the call centers and the website has been improved to handle the large number of visitors. Still, the rollout of these resources should have been far better, and I regret that the response exacerbated rather than alleviated matters for so many.

#### **How It Happened**

First and foremost, I want to respond to the question that is on everyone's mind, which is, "How did this happen?" In my testimony, I will address both what I learned and did at key times in my role as CEO, and what I have since learned was occurring during those times, based on the company's ongoing investigation. Chronologically, the key events are as follows:

On March 8, 2017, the U.S. Department of Homeland Security, Computer Emergency Readiness Team ("U.S. CERT") sent Equifax and many others a notice of the need to patch a particular vulnerability in certain versions of software used by other businesses. Equifax used that software, which is called "Apache Struts," in its online disputes portal, a website where consumers can dispute items on their credit report.



On March 9, Equifax disseminated the U.S. CERT notification internally by email requesting that applicable personnel responsible for an Apache Struts installation upgrade their software. Consistent with Equifax's patching policy, the Equifax security department required that patching occur within a 48 hour time period. We now know that the vulnerable version of Apache Struts within Equifax was not identified or patched in response to the internal March 9 notification to information technology personnel.

On March 15, Equifax's information security department also ran scans that should have identified any systems that were vulnerable to the Apache Struts issue identified by U.S. CERT. Unfortunately, however, the scans did not identify the Apache Struts vulnerability. Equifax's efforts undertaken in March 2017 did not identify any versions of Apache Struts that were subject to this vulnerability, and the vulnerability remained in an Equifax web application much longer than it should have. I understand that Equifax's investigation into these issues is ongoing. The company knows, however, that it was this unpatched vulnerability that allowed hackers to access personal identifying information.

Based on the investigation to date, it appears that the first date the attacker(s) accessed sensitive information may have been on May 13, 2017. The company was not aware of that access at the time. Between May 13 and July 30, there is evidence to suggest that the attacker(s) continued to access sensitive information, exploiting the same Apache Struts vulnerability. During that time, Equifax's security tools did not detect this illegal access.

On July 29, however, Equifax's security department observed suspicious network traffic associated with the consumer dispute website (where consumers could investigate and contest issues with their credit reports). In response, the security department investigated and immediately blocked the suspicious traffic that was identified. The department continued to monitor network traffic and observed additional suspicious activity on July 30, 2017. In response, they took the web application completely offline that day. The criminal hack was over, but the hard work to figure out the nature, scope, and impact of it was just beginning.

I was told about the suspicious activity the next day, on July 31, in a conversation with the Chief Information Officer. At that time, I was informed that there was evidence of suspicious activity on our dispute portal and that the portal had been taken offline to address the potential issues. I certainly did not know that personal identifying information ("PII") had been stolen, or have any indication of the scope of this attack.

On August 2, consistent with its security incident response procedures, the company: 1) retained the cybersecurity group at the law firm of King & Spalding LLP to guide the investigation and provide legal and regulatory advice; 2) reached out, through company counsel, to engage the independent cybersecurity forensic consulting firm, Mandiant, to investigate the suspicious activity; and 3) contacted the Federal Bureau of Investigation ("FBI").

Over the next several weeks, working literally around the clock, Mandiant and Equifax's security department analyzed forensic data seeking to identify and understand unauthorized activity on the network. Their task was to figure out what happened, what parts of the Equifax network were affected, how many consumers were affected, and what types of information was

accessed or potentially acquired by the hackers. This effort included identifying and analyzing available forensic data to assess the attacker activity, determining the scope of the intrusion, and assessing whether the intrusion was ongoing (it was not; it had stopped on July 30 when the portal was taken offline). Mandiant also helped examine whether the data accessed contained personal identifying information; discover what data was exfiltrated from the company; and trace that data back to unique consumer information.

By August 11, the forensic investigation had determined that, in addition to dispute documents from the online web portal, the hackers may have accessed a database table containing a large amount of consumers' PII, and potentially other data tables.

On August 15, I was informed that it appeared likely that consumer PII had been stolen. I requested a detailed briefing to determine how the company should proceed.

On August 17, I held a senior leadership team meeting to receive the detailed briefing on the investigation. At that point, the forensic investigation had determined that there were large volumes of consumer data that had been compromised. Learning this information was deeply concerning to me, although the team needed to continue their analysis to understand the scope and specific consumers potentially affected. The company had expert forensic and legal advice, and was mindful of the FBI's need to conduct its criminal investigation.

A substantial complication was that the information stolen from Equifax had been stored in various data tables, so tracing the records back to individual consumers, given the volume of records involved, was extremely time consuming and difficult. To facilitate the forensic effort, I approved the use by the investigative team of additional computer resources that significantly reduced the time to analyze the data.

On August 22, I notified Equifax's lead member of the Board of Directors, Mark Feidler, of the data breach, as well as my direct reports who headed up our various business units. In special telephonic board meetings on August 24 and 25, the full Board of Directors was informed. We also began developing the remediation we would need to assist affected consumers, even as the investigation continued apace. From this point forward, I was updated on a daily – and sometimes hourly – basis on both the investigative progress and the notification and remediation development.

On September 1, I convened a Board meeting where we discussed the scale of the breach and what we had learned so far, noting that the company was continuing to investigate. We also discussed our efforts to develop a notification and remediation program that would help consumers deal with the potential results of the incident. A mounting concern also was that when any notification is made, the experts informed us that we had to prepare our network for exponentially more attacks after the notification, because a notification would provoke "copycat" attempts and other criminal activity.

By September 4, the investigative team had created a list of approximately 143 million consumers whose personal information we believed had been stolen, and we continued our planning for a public announcement of a breach of that magnitude, which included a rollout of a

comprehensive support package for consumers. The team continued its work on a dedicated website, [www.equifaxsecurity2017.com](http://www.equifaxsecurity2017.com), where consumers could learn whether they were impacted and find out more information, a dedicated call center to assist consumers with questions, and a free credit file monitoring and identity theft protection package for all U.S. consumers, regardless of whether they were impacted.

I understand that Equifax kept the FBI informed of the progress and significant developments in our investigation, and felt it was important to notify the FBI before moving forward with any public announcement. We notified the FBI in advance of the impending notification.

On September 7, 2017, Equifax publicly announced the breach through a nationwide press release. The release indicated that the breach impacted personal information relating to 143 million U.S. consumers, primarily including names, Social Security numbers, birth dates, addresses and, in some instances, driver's license numbers.

These are the key facts as I understand them. I also understand that the FBI's investigation and Equifax's own review and remediation are ongoing, as are, of course, numerous other investigations.

#### **Protecting U.S. Consumers Affected by the Breach**

From the third week in August, when it became clear that our worst fears had come true and Equifax had experienced a significant breach, my direction was to continue investigating but first and foremost to develop remediation to protect consumers from being harmed and comply with all applicable notification requirements, based on advice of outside cybersecurity counsel and Mandiant. Significantly, a major task was the need to deploy additional security measures across the entire network because we were advised that as soon as Equifax announced the hack, there would be a dramatic increase in attempted hacking. There were three main components to Equifax's plan: 1) a website where consumers could look up if they were affected by the breach and then register for a suite of protective tools; 2) a call center to answer questions and assist with registration; 3) the package of tools themselves that the company was offering to everyone in the country. The task was massive – Equifax was preparing to explain and offer services to every American consumer.

First, a new website was developed to provide consumers with additional information – beyond the press release – about the nature, extent, and causes of the breach. This was extremely challenging given that the company needed to build a new capability to interface with tens of millions of consumers, and to do so in less than two weeks. That challenge proved overwhelming, and, regrettably, mistakes were made. For example, terms and conditions attached to the free solutions that Equifax offered included a mandatory arbitration clause. That provision – which was never intended to apply in the first place – was immediately removed as soon as it was discovered. (I was informed later that it had simply been inadvertently included in terms and conditions that were essentially “cut and pasted” from a different Equifax offering.)

The initial rollout of Equifax's call centers had frustrating shortcomings as well. Put simply, the call centers were confronted by an overwhelming volume of callers. Before the breach, Equifax had approximately 500 customer service representatives dedicated to consumers, so the company needed to hire and train thousands more, again in less than two weeks. To make matters worse, two of the larger call centers in Florida were forced to close for a period of time in the wake of Hurricane Irma. The closure of these call centers led to a reduction in the number of available customer service representatives and added to the already significant wait times that callers experienced. Many needlessly waited on hold or were otherwise unable to have their questions answered through the call centers, which I deeply regret. My understanding is that the call centers are now fully functional. The number of customer service representatives, which is now over 2,500, continues to increase, and I am informed that wait times have decreased substantially.

Beyond the website and the call centers, the company also developed a comprehensive support package for all American consumers, regardless of whether they were directly affected by the incident or not, that includes free: 1) credit file monitoring by all three credit bureaus; 2) Equifax credit lock; 3) Equifax credit reports; 4) identity theft insurance; and 5) Social Security Number "dark web" scanning for one year. Importantly, enrolling in the program is free, and will not require consumers to waive any rights to take legal action for claims related to the free services offered in response to the cybersecurity incident or for claims related to the cybersecurity incident itself.

Despite these challenges, it appears that Equifax's efforts are reaching many people. As of late September, the website had received over 420 million hits. And similarly, as of late September, over 7.5 million activation emails have been sent to consumers who registered for the program.

Equifax also recently announced a new service that I understand will be available by January 31, 2018, that will allow consumers to control their own credit data, by allowing them to lock and unlock their credit files at will, repeatedly, for free, for life. I was pleased to see the company move forward with this plan, which we had put in motion months ago, and which I directed the company to accelerate, as we were constructing the remedial package in response to the breach.

The hard work of regaining the trust of the American people that was developed over the course of the company's 118 year history is ongoing and must be sustained. I believe the company, under the leadership of Lead Director Mark Feidler, and interim CEO Paulino do Rego Barros, Jr. will continue these efforts with vigor and commitment.

#### **How to Protect Consumer Data Going Forward**

It is extremely important that notwithstanding the constant threat of cybercriminals, the American people and the Members of this Committee know that Equifax is doing everything in its power to prevent a breach like this from ever happening again. Since the potential breach was discovered, those inside and outside the company have worked around-the-clock to enhance the Company's security measures. While I am limited in what I can say publicly about these specific

measures, and going forward these questions are best directed to new management, I want to highlight a few steps that Equifax has already taken to better protect consumer data moving forward, including the website developed to respond to the hack, and some changes still to come.

In recent weeks, vulnerability scanning and patch management processes and procedures were enhanced. The scope of sensitive data retained in backend databases has been reduced so as to minimize the risk of loss. Restrictions and controls for accessing data housed within critical databases have been strengthened. Network segmentation has been increased to restrict access from internet facing systems to backend databases and data stores. Additional web application firewalls have been deployed, and tuning signatures designed to block attacks have been added. Deployment of file integrity monitoring technologies on application and web servers has been accelerated. The company is also implementing additional network, application, database, and system-level logging. These are just a few of the steps Equifax has taken in recent weeks to shore up its security protocols.

Importantly, Equifax's forensic consultants have recommended a series of improvements that are being installed over the next 30, 60, and 90 day periods, which the company was in the process of implementing at the time of my retirement. In addition, at my direction a well-known, independent expert consulting firm (in addition to and different from Mandiant) has been retained to perform a top-to-bottom assessment of the company's information security systems.

Beyond the recent technological enhancements, Equifax has also made several strategic personnel changes at the highest levels of the company. Accountability starts at the top and I, therefore, decided to step down as CEO and retire early to allow the company to move forward. Before I retired, our Chief Information Officer and Chief Security Officer also left the company. Equifax's interim appointments for each of these positions, including Paulino do Rego Barros, Jr., the interim CEO, are ready, able and qualified to step into their new roles and to help consumers, and the company, recover from this regrettable incident.

It is my hope and expectation that, at the conclusion of the investigation, we will have an even more complete account of what happened, how future attacks by criminal hackers can be deterred and suspicious activity curbed more quickly, and most importantly, how consumers' concerns about the security of their personal data can be alleviated.

#### **Toward a New Paradigm in Data Security**

Where do we go from here? Although I have had little time for reflection regarding the awful events of the last few weeks, this humbling experience has crystalized for me two observations: First, an industry standard placing control of access to consumers' credit data in the hands of the consumers should be adopted. Equifax's free lifetime lock program will allow consumers, and consumers alone, to decide when their credit information may be accessed. This should become the industry standard. Second, we should consider the creation of a public-private partnership to begin a dialogue on replacing the Social Security Number as the touchstone for identity verification in this country. It is time to have identity verification procedures that match the technological age in which we live.

The list of companies and government agencies that have suffered major hacks at the hands of sophisticated cybercriminals is sadly very long, and growing. To my profound disappointment, Equifax now finds itself on that list. I have stepped away from a company I have led and loved and help build for more than a decade. But I am not stepping away from this problem and I am strongly committed to helping address the important questions this episode has raised. Part of that starts today, as I appear at this hearing and others voluntarily to share what I know. Going forward, however, government and the private sector need to grapple with an environment where data breaches will occur. Giving consumers more control of their data is a start, but is not a full solution in a world where the threats are always evolving. I am hopeful there will be careful consideration of this changing landscape by both policymakers and the credit reporting industry.

#### **Conclusion**

Chairman Hensarling, Ranking Member Waters, and Honorable Members of the Committee, thank you again for inviting me to speak with you today. I will close by saying again how so sorry I am that this data breach occurred. On a personal note, I want to thank the many hard-working and dedicated people who worked with me for the last 12 years, and especially over the last eight weeks, as we struggled to understand what had gone wrong and to make it right. This has been a devastating experience for the men and women of Equifax. But I know that under the leadership of Paulino and Mark they will work tirelessly, as we have in the past two months, to making things right.

I realize that what I can report today will not answer all of your questions and concerns, but I can assure you and the American public that I will do my level best to assist you in getting the information you need to understand this incident and to protect American consumers.



We're the Consumer Financial Protection Bureau (CFPB), a U.S. government agency that makes sure banks, lenders, and other financial companies treat you fairly.

[Learn how the CFPB can help you](#)

UPDATED JUN 01, 2017

## How can I spot identity theft?

**Answer:** Keep an eye out for identity theft by reading your statements from credit card companies or banks and credit unions and checking your credit reports for suspicious activity.

### Financial accounts and billing statements

Look closely for charges you did not make. Even a small charge can be a danger sign. Thieves sometimes will take a small amount from your checking account and then return to take much more if the small debit goes unnoticed.

### Credit reports

Review your free credit reports from each of the three major credit bureaus. If an identity thief is opening financial accounts in your name, these accounts may show up on your credit report. Look for:

- Inquiries from companies you've never contacted
- Accounts you didn't open
- Wrong amounts on your accounts

### TIP:

Be sure your personal information – like your Social Security number, address, name or initials, and employers – is correct.

**Warning: Don't ignore bills from people you don't know.** A bill on a debt you never borrowed may be an indication that someone else has opened an account in your name. Contact the creditor to find out.

If you have a problem with credit reporting, you can [submit a complaint](#).



---

We're the Consumer Financial Protection Bureau (CFPB), a U.S. government agency that makes sure banks, lenders, and other financial companies treat you fairly.

[Learn how the CFPB can help you](#)

---

UPDATED MAR 28, 2017

## What is identity theft?

**Answer:** Identity theft occurs when someone steals your identity to commit fraud.

Stealing your identity could mean using personal information without your permission, such as:

- Your name
- Social Security number
- Credit card number

Identity thieves may rent apartments, get credit cards, or start other accounts in your name. You may not find out about the theft until you [review your credit report](#) or a credit card statement and notice accounts you didn't open, charges you didn't make, or until you're contacted by a debt collector.

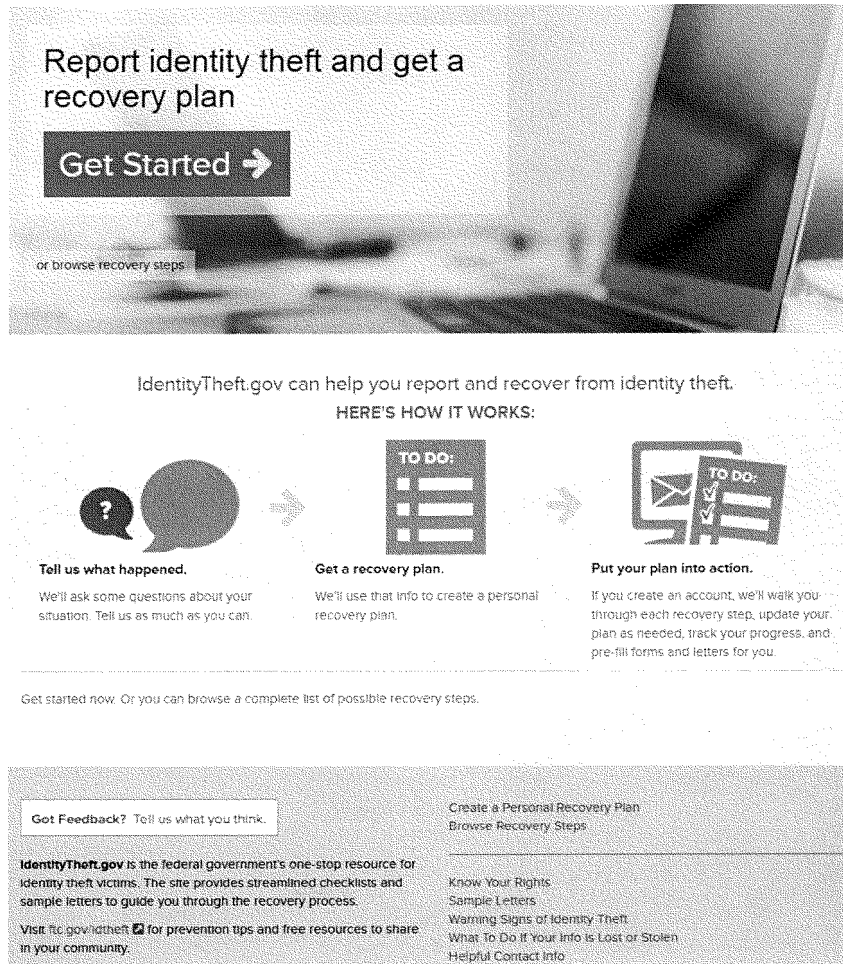
---

**TIP:**

Learn how you can [spot identity theft](#) and visit [IdentityTheft.gov](#), the federal government's one-stop resource to help you report and recover from identity theft.

---






**Report identity theft and get a recovery plan**

**Get Started →**

or browse recovery steps


IdentityTheft.gov can help you report and recover from identity theft.

**HERE'S HOW IT WORKS:**




**Tell us what happened.**

We'll ask some questions about your situation. Tell us as much as you can.



**Get a recovery plan.**

We'll use that info to create a personal recovery plan.



**Put your plan into action.**

If you create an account, we'll walk you through each recovery step, update your plan as needed, track your progress, and pre-fill forms and letters for you.

Get started now. Or you can browse a complete list of possible recovery steps.

**Got Feedback?** Tell us what you think.

**IdentityTheft.gov** is the federal government's one-stop resource for identity theft victims. The site provides streamlined checklists and sample letters to guide you through the recovery process.

Visit [ic.gov/idtheft](http://ic.gov/idtheft) for prevention tips and free resources to share in your community.

**Create a Personal Recovery Plan**  
Browse Recovery Steps

Know Your Rights  
Sample Letters  
Warning Signs of Identity Theft  
What To Do If Your Info Is Lost or Stolen  
Helpful Contact Info

Source: <https://www.identitytheft.gov/>

