AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

S. HRG. 115–129

AN EXAMINATION OF THE EQUIFAX CYBERSECURITY BREACH

HEARING

BEFORE THE

COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS UNITED STATES SENATE

ONE HUNDRED FIFTEENTH CONGRESS

FIRST SESSION

ON

EXAMINING THE EQUIFAX CYBERSECURITY BREACH AND ITS IMPACT ON APPROXIMATELY 143 MILLION U.S. CONSUMERS

OCTOBER 4, 2017

Printed for the use of the Committee on Banking, Housing, and Urban Affairs

Available at: http://www.govinfo.gov/

U.S. GOVERNMENT PUBLISHING OFFICE
28–123 PDF WASHINGTON : 2018

For sale by the Superintendent of Documents, U.S. Government Publishing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS

MIKE CRAPO, Idaho, *Chairman*

RICHARD C. SHELBY, Alabama	SHERROD BROWN, Ohio
BOB CORKER, Tennessee	JACK REED, Rhode Island
PATRICK J. TOOMEY, Pennsylvania	ROBERT MENENDEZ, New Jersey
DEAN HELLER, Nevada	JON TESTER, Montana
TIM SCOTT, South Carolina	MARK R. WARNER, Virginia
BEN SASSE, Nebraska	ELIZABETH WARREN, Massachusetts
TOM COTTON, Arkansas	HEIDI HEITKAMP, North Dakota
MIKE ROUNDS, South Dakota	JOE DONNELLY, Indiana
DAVID PERDUE, Georgia	BRIAN SCHATZ, Hawaii
THOM TILLIS, North Carolina	CHRIS VAN HOLLEN, Maryland
JOHN KENNEDY, Louisiana	CATHERINE CORTEZ MASTO, Nevada

GREGG RICHARD, *Staff Director*
MARK POWDEN, *Democratic Staff Director*

ELAD ROISMAN, *Chief Counsel*
JOE CARAPIET, *Senior Counsel*
BRANDON BEALL, *Professional Staff Member*

ELISHA TUKU, *Democratic Chief Counsel*
LAURA SWANSON, *Democratic Deputy Staff Director*
COREY FRAYER, *Democratic Professional Staff Member*

DAWN RATLIFF, *Chief Clerk*
CAMERON RICKER, *Deputy Clerk*
JAMES GUILIANO, *Hearing Clerk*
SHELVIN SIMMONS, *IT Director*
JIM CROWELL, *Editor*

C O N T E N T S

WEDNESDAY, OCTOBER 4, 2017

WITNESS

ADDITIONAL MATERIAL SUPPLIED FOR THE RECORD

AN EXAMINATION OF THE EQUIFAX CYBERSECURITY BREACH

WEDNESDAY, OCTOBER 4, 2017

U.S. SENATE,
COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS
Washington, DC.

The Committee met at 10:03 a.m., in room SD–538, Dirksen Senate Office Building, Hon. Michael Crapo, Chairman of the Committee, presiding.

OPENING STATEMENT OF CHAIRMAN MIKE CRAPO

Chairman CRAPO. This Committee will come to order.

This morning, we will hear testimony from Richard Smith, former chairman and chief executive officer of Equifax, who held those positions until last week.

I understand that you are now serving as an unpaid advisor to the company and appreciate your willingness to testify here and appear and testify about the events surrounding the breach and Equifax's response while you were leading the company.

Given the severity of this data breach, Congress will continue to examine the facts behind it and what can be done to prevent similar situations.

Cybersecurity is one of the most pressing issues facing companies, as well as consumers and Governments alike, and is one of the biggest threats to our financial system. The amount of data that the private industry and Government collect and store is very concerning. There is intrinsic vulnerability in collecting and storing personal financial information, and we need to have a meaningful discussion on how to protect and limit access to it.

The Banking Committee takes its oversight of credit bureaus seriously, as they are financial institutions under the Gramm–Leach–Bliley Act.

Credit bureaus serve a critical function in our financial system and have become a daily part of every American's life. Every day, these institutions intersect in people's attempts to get credit cards, car loans, mortgages, and other items.

Consumers may know about their involvement in their lives, such as when they directly request a credit report, but sometimes they do not, like when a company requests a background check to determine their eligibility for a cell phone.

The ability of Americans to easily access credit is one of the many things that make our economy and our country the envy of the world. It is also why this breach is so shocking and concerning.

Here is what we know based on information from Equifax. Equifax experienced a cybersecurity breach which potentially impacted more than 145 million U.S. consumers. The data that was taken included the names, Social Security numbers, birth dates, addresses, and in some cases driver's license numbers.

In addition, credit card numbers for approximately 209,000 consumers and dispute documents with personally identifiable information for approximately 182,000 consumers were accessed.

According to Equifax, the unauthorized access took place from mid-May through July 2017, with Equifax discovering the situation on July 29 and then finally cutting off the intruders.

Here is what we need to know. Why did it take Equifax 6 weeks from the time it learned of the breach to tell the public, the regulators, and the 145 million American victims about it? Why were Equifax executives trading during this time? How strong were and are Equifax's cybersecurity practices?

After the breach, what interactions did the company have with other credit bureaus and Government agencies, in order to understand what, if anything, can be improved in terms of information sharing and mitigating consumer harm?

Additionally, there are valid and important questions about the steps Equifax has taken to remediate customers and whether more needs to be done to minimize the potential harm to those affected.

In an op-ed last week, your successor admitted that answers to key consumer questions were often delayed, incomplete, or both. That same op-ed asserted that it is important to give consumers the power to protect and control access to their personal credit data.

I look forward to having these questions answered and exploring different options on how companies can better safeguard consumers' information.

Senator Brown.

OPENING STATEMENT OF SENATOR SHERROD BROWN

Senator BROWN. Thank you, Chairman Crapo.

The story of this data breach is a familiar one. A big financial institution screwed up. Executives walk away with millions of dollars. Tens of millions of Americans end up holding the bag.

Unfortunately, Americans have come to expect that the Equifax scandal will play out the same way as the Wells Fargo scandal. A couple executives retire. Some of them lose some of their bonuses. A couple fines are issued, and only later do we find out the problems go much, much deeper.

Most Americans never chose to have their data scooped up by Equifax. You have said that since 2005, Equifax has been rapidly transforming itself into a—your words—"global analytics company" by collecting huge troves of information on people that you can sell to marketers and employers, but you almost never ask people if they want to be tracked.

Most of the 145 million people—that number seems to climb every week or so—well over half of all adults in the United States, most of the 145 million people whose data you allowed to be stolen probably only had a vague idea of what Equifax was, if they had

heard of you at all. Then they read in the paper that their personal information has, in fact, been compromised.

But while they might not have known the name Equifax, they should have been able to expect that a company that gathers the most private information about them would have state-of-the-art protections for that information. A gold mine for hackers should be a digital Fort Knox when it comes to security.

But security does not generate short-term profits. Protecting consumers apparently is not important to your business model, so you gathered more and more information. You peddled it to more and more buyers.

For example, you bought a company called TALX so you could get access to detailed payroll information—the hours people worked, how much they were paid, even where they lived—7,000 businesses.

You were hacked there, too, exposing the workers of one proud Ohio company, 400,000 workers at Kroger, and an unknown number of people's information to criminals who used it to commit tax fraud.

In May of this year, your outside law firm stated that Equifax had instituted additional security measures in order to prevent a recurrence of the TALX incident, just like you are claiming you are doing now. Yet at that same time, hackers had already taken advantage of another security flaw to get into Equifax's system.

It has been 10 weeks since you discovered this latest breach, but I still do not think we have a complete answer to the question what happened and why.

We do know that this breach could have been avoided if you had taken the simple step of administering security patches, but your response after the fact may have been just as negligent.

You told the House yesterday that Equifax knew at least some people's data had been exposed on August 15th. Rather than giving victims a chance to protect themselves, you withheld this information from the public for weeks.

You claim that you delayed telling the public about this hack so you could get an appropriate consumer response put together, but when you finally did tell people what happened, Equifax's website and call centers were immediately overwhelmed.

You even tried to take advantage of the situation by sticking victims with a forced arbitration clause buried in the credit monitoring product you were shopping to victims. Think about that. You tried to take advantage further, even with all this, when the public was so upset because you had betrayed their trust and the public trust. You stick the victims with a forced arbitration clause buried in the credit monitoring product you were shopping to victims. At least in this instance, you backed down under public pressure, unlike Wells Fargo, which yesterday under withering questions continued to resist.

Chairman Crapo and I sent a letter to you on September 22nd requesting basic information. For example, is there a company policy on stock sales? I would guess so, but the best we got from the company was, quote, "Equifax will work with Committee staff to provide a copy of the policy," unquote. We are not talking about trade secrets here. I just do not get the obfuscation.

Despite your promise to deliver a free CreditLock product next year, all of Equifax's actions up to this point demonstrate that this simply is not a company that deserves to be trusted with Americans' personal data.

Your actions have exposed over half the country's adults to financial harm. Equifax has forfeited its right to corporate secrets. So please do not make the same mistake that Wells Fargo did. Now is the time to give this Committee the whole story.

Thank you, Mr. Chairman.

Chairman CRAPO. Thank you, Senator Brown.

And now we will proceed to the testimony. We will hear testimony from Mr. Richard Smith, former chairman and chief executive officer of Equifax, Inc.

Mr. Smith, your written statement will be made a part of the record in its entirety, and you may proceed with your oral remarks.

STATEMENT OF RICHARD F. SMITH, FORMER CHAIRMAN AND CHIEF EXECUTIVE OFFICER, EQUIFAX, INC.

Mr. SMITH. Thank you, and good morning. Thank you, Chairman Crapo, Ranking Member Brown, and Honorable Members of the Committee. Thank you for the opportunity to testify before you this morning.

My name again is Rick Smith, and for the last 12 years, I have had the honor of serving as chairman and CEO as Equifax. As noted, I have submitted written testimony, which addresses the details of my testimony in far more detail than I will get in my oral comments.

I have talked to many consumers, and I have read their letters. I understand how frustrated and fearful many Americans are about what happened at Equifax. This criminal attack took place on my watch, and I take full responsibility as CEO at the time. I want to say to every American, I am truly and deeply sorry for what happened.

Americans have the right to know how this happened, and I am prepared to testify today about what I learned and what I did about the incident and my role as CEO and chairman of the board and also what I know and what I have learned about the incident as a result of being briefed by the company's investigation, which is ongoing.

As we now know, this criminal attack was made possible because a combination of a human error and a technological error. The human error involved the failure to apply a patch to our dispute portal in March of 2017. The technological error involved a scanner, which failed to detect the vulnerability on this particular portal, which had not been patched. Both errors have since been addressed.

On July 29th and July 30th, suspicious activity was detected. We followed our security incident response protocol at that time. The team immediately shut down the portal and began our internal security investigation.

On August 2nd, we hired top security, cybersecurity, forensic, and legal experts, and we notified the FBI. At that time, we did not know the nature or the scope of the incident.

It was not until late August that we concluded that we had experienced a major data breach.

Over the weeks leading up to September 7th, our team continued working around the clock to prepare to make things right. We took four steps to protect consumers: first, determining when and how to notify the public, relying on the advice of our experts that we needed to have a plan in place as soon as we announced; two, helping consumers by developing a website and staffing up a mass of call centers and offering free services to every American; three, preparing for increased cyberattacks, which we were advised are common after the notice of a breach; and finally, number four, continue to coordinate with the FBI and their criminal investigation of the hackers and notifying other Federal and State agencies.

In the rollout of our remediation program, mistakes were made for which again I am deeply apologetic. I regret the frustration that many Americans felt when our websites and call centers were overwhelmed in the early weeks. It is no excuse, but it certainly did not help that two of our larger call centers were shut down for days by Hurricane Irma.

Since then, however, the company has dramatically increased its capacity, and I can report to you today that we have handled more than 420 million consumer visits to our website, and the wait time at our call centers have been dramatically reduced.

At my direction, the company offered a broad package of service offerings to all Americans, all of them free to help protect consumers.

In addition, we developed a new service that will be available January 31st, 2018, that will give all consumers the power to control access to their credit data by allowing them to lock and unlock their credit files whenever they want for free and for life, putting the power to control access to data in the hands of the American consumer. I am looking forward to discussing this tool with you in detail during my testimony.

As we have all painfully learned, data security is a national security problem. Putting consumers in control of their credit data is a first step toward a long-term solution to the problem of identity theft.

But no single company could solve the larger problem on its own. I believe we need a public–private partnership to evaluate how to best protect American consumers' personal data ongoing. I look forward to being a part of that dialogue.

Chairman Crapo, Ranking Member Brown, and the Honorable Members of the Committee, thank you again for inviting me to speak before you today.

I will close again by saying how sorry I am about this breach. On a personal note, I want to thank the many hardworking and dedicated people who have worked with me so tirelessly over the last 12 years. Equifax is a very good company with thousands of great people trying to do the right thing each and every day. I know that they will continue to work tirelessly, as we have over the past few months to right this wrong.

Thank you.

Chairman CRAPO. Thank you, Mr. Smith.

Mr. Smith, you recently discussed the need to give consumers control of their own data. Yesterday, you said, "It is time we change the paradigm, give the power back to the consumer to control who accesses his or her credit data. It is the right thing to do."

But we are far from that reality today with credit bureaus. First, what needs to be changed to give consumers this power?

Mr. SMITH. Mr. Chairman, the start is this product we are introducing, which will come out in January of next year, which gives the consumer the ability to control who and when accesses the credit data. It will be a simple tool, Web-enabled on an application, and the consumer can simply dictate who gets access, who does not, and if he or she wants to go to a bank to get a credit card or a car loan, they simply can toggle on, open the access for the underwriter to look at their credit file, once complete, toggle off, and secure.

Chairman CRAPO. And it seems to me if that solution works that that is a solution or a part of the solution with regard to other private-sector actors or illegal actors. What about the Government? Does the Federal Reserve or the CFPB have access to your data, to Equifax's data?

Mr. SMITH. Sir, Mr. Chairman, if a consumer locks their—at the consumer level, is that the question?

Chairman CRAPO. Yes.

Mr. SMITH. If the consumer locks their file, they lock out anyone's access to that data.

Chairman CRAPO. So you are not in a position of being required by any Federal agency to provide this personally identifiable data to that agency?

Mr. SMITH. Mr. Chairman, I am not sure I understand the question. If a consumer locks their file to prevent access to their file from any other bank or telecommunications company, they would be the only ones who could unlock that file. We could not unlock that file on their behalf, if I understand the question correctly.

Chairman CRAPO. Even if asked by a Government agency as opposed to an inquiring bank?

Mr. SMITH. I would have to check that.

Chairman CRAPO. All right. Thank you. I would appreciate that.

Mr. SMITH. Thank you.

Chairman CRAPO. In the hearing yesterday, you mentioned that we may need to think about how secure Social Security numbers really are and if they are really the best identifier going forward for consumers. Could you give us your thoughts on that?

Mr. SMITH. Yes. Mr. Chairman, I worry about the fact that Social Security numbers have been out there since 1936 and used to be on our driver's license and used in our employment. You talked to many cybersecurity experts, and they say they vast majority of all SSNs have already been compromised.

I am in no way skirting the issue of the horrific breach that we had. It was horrific, and I once again apologize to this Committee and to all Americans. But I would encourage a dialogue to talk about what is a better way to identify individuals, something beyond the SSN.

Chairman CRAPO. Do you have any ideas as to what that might be, what could we effectively transfer into?

Mr. SMITH. I do not, but I would love to be part of that dialogue, the combination of public and private partnership with academic, to think about that. There is a lot of thinking going on right now. I am sure with the right thought and a priority, we could crack that code.

Chairman CRAPO. All right. Thank you.

There have been some issues and confusion relating to the product you just discussed and services that Equifax has offered in light of the breach. Some of my constituents have said they are having trouble gaining access to the remediation products being offered. What exactly are customers being offered today, and what do they need to do to obtain these products and services?

Mr. SMITH. Thank you.

We are offering five different services for free, and to repeat, this is to all Americans, not just the victims of the criminal attack.

Number one, it is a three-bureau monitoring, where you can monitor activity against your credit file from ourselves, TransUnion, and Experian. Two is the ability to lock the file. Number three is the ability to scan. We scan the dark web on behalf of the consumer looking for Social Security activity that might occur. Number four is access to our file for free, and number five is an insurance product that helps recoup costs up to a million dollars if a consumer has costs in trying to fight, repair their credit.

So those are the five services we offer today to all Americans, and the other, Chairman, is the one we talked about that is available in 2018, January 31st of 2018, which is the next generation of Lock.

Chairman CRAPO. All right. Thank you very much.

Senator Brown.

Senator BROWN. Thank you, Mr. Chairman.

According to your testimony in the House yesterday, over the last 3 years, you have spent $250 million on cybersecurity. That is about $85 million a year, correct?

Mr. SMITH. Yes. That was an estimate that over the last 3 years, it is approaching a quarter billion dollars.

Senator BROWN. And since 2016, you have made personally about $69 million; is that correct?

Mr. SMITH. I have not tracked that number, to be honest.

Senator BROWN. In hindsight, do you think Equifax should have spent more money protecting people's data rather than compensating you so well?

Mr. SMITH. I look back at the money we have spent. It is not a matter of the dollars spent. It was not a financial constraint, by any means. Obviously, when you look at the issue in hindsight, it is could you have spent money differently, not the total dollars spent.

There is a benchmark out there that was done by IBM that benchmarks financial services company, and their total security spend is a percent of IT. And their benchmark talks about a range of 10 to 14 percent. Our range is in the range of 12 percent. So, again, we are spending money in a range that——

Senator BROWN. Well, I am going to interrupt you because I know that in the House, House hearing, there were not nearly as many questions because your answers were pretty long, and I un-

derstand the complexities of this. But you are an IT company, and that is just not acceptable.

Last August, this past August at a business school event at the University of Georgia, you bragged that Equifax gets its data basically cost-free. You were also asked how you approach data fraud, and you responded, quote, "Fraud is a huge opportunity for us." Your SEC filings back that up. They state that a significant portion of your revenue comes from selling credit monitoring and fraud protection services to consumers. So do you think, Mr. Smith, it is fair that Equifax gets to take its consumers' data at almost no cost, make millions by selling it to data-mining companies and marketers, then charge fees to those consumers for credit monitoring products after they become identity theft victims?

Mr. SMITH. Senator, the vast majority of what we do is allowing consumers to get access to credit. We take their data combined with analytics and allow underwriters at banks, credit card lenders, automotive lenders, to make loans to consumers. We make very little money as a percent of our total revenue from selling monitoring products to consumers.

Senator BROWN. But the point is you keep making money off people's sensitive data either way.

Equifax does not get its data directly from consumers, as you know, and as several on this Committee have pointed out, it gets it from their banks, their utility companies, their employers, all without consent of the borrowers and the employees.

Congress long ago, as I think you know, decided that companies could not traffic in people's medical records for obvious and good reason and that they needed to consent to a transfer. Why should not we do the same with financial records? You know how important that personal financial data is to people. Why not do the same with financial records? Do you think we need to change the consumer reporting industry in this country to give Americans ownership of the data? For example, should they be allowed to request that you delete the data from your systems?

Mr. SMITH. Senator, two thoughts. One is we are a vital part to the global economy. We provide a great service to the consumer enabling them to get access to credit.

We also enable the unbanked because of our data to have the opportunity to get into the credit market. So it is a vital and very important role we play and have played for many, many years.

Yes, there are things we can do better as an industry and working with Government, and the one thing I would like to see us talk about as an industry is this concept of giving the consumer the power to control their data. One small step forward is the concept of this lock for life. I would like to see the entire industry move in that direction.

Senator BROWN. I am trying to read between the lines. Is that a yes or a no to the question of should consumers be allowed to request you delete their data from your system, their data that you gather without their knowledge?

Mr. SMITH. I believe a better way to get at that is through this lock concept.

Senator BROWN. So that means no?

Mr. SMITH. Correct.

Senator BROWN. Even though we do it with medical data and even though—I mean, fundamentally, if you do not think consumers should be allowed to control their own data, the question is why should a company that has had so many security failures be allowed to control their data. That is the fundamental question that this company has not—apparently has not asked or certainly has not answered to the public.

Thank you.

Chairman CRAPO. Thank you.

And I would note to the Senators that Senator Brown and I both stayed within our 5 minutes. I encourage all of you to follow that pattern.

Senator SASSE. It was kind of impressive.

Senator KENNEDY. It was kind of unusual.

[Laughter.]

Chairman CRAPO. Senator——

Senator SASSE. I think it is me. Yeah.

Chairman CRAPO. ——Sasse.

Senator SASSE. Thank you, Chairman.

Mr. Smith, let us take a minute to talk about why we are here. Big picture, it is this. There is a really small group of credit bureaus in America, and by really small, I mean three. And if you are an American who buys a home or a car, you typically have to be cleared by one of those three, and even if you do not have a relationship with one of the three, if you are a consumer who did not choose this, so you think about the OPM hack, people were at least choosing to apply for a security clearance or to work for the Federal Government. We have people here who did not have any relationship with you and did not choose to engage with you.

If you get a credit card from one of the countless offers that Americans get every day in their mailbox from department stores or gas stations or airlines, it is not uncommon for one of the three credit bureaus to then obtain your information. So what happens when something goes wrong? What happens when one of you big three is hacked? What happens if you are one of the 145 million Americans who, in this case, had their information stolen? What happens if 5 years from now an American has their identity information stolen? What happens when there is a reasonable suspicion that folks at your organization may have engaged in insider trading?

There is a lot of anxiety that Americans feel, and they are Americans who do not have the benefit of powerful attorneys and lobbyists. And for them, this hearing is one of their only shots at getting a full account of what went wrong, who is to blame, and what is going to happen about it in the future.

So I would like to discuss this question about those who were impacted by the breach and how long you think Equifax's exposure or responsibility lasts. If you are an American, if you are one of those 145 million, you do not have the ability to change your name, your mother's maiden name, your birth date, your Social Security number, and your organization has committed to providing identity monitoring services for the next year.

But I am curious about whether or not Equifax and your board have deliberated. Do you think your responsibility ends in 1 year,

in 2 years, in 5 years, in 10 years? And if you think it ends at some point, have you tried to think about the goodwill and balance sheet impact of all this? How can you explain to an American whose identity might be stolen later, because of this breach, why your responsibility would ever end? Does it end?

Mr. SMITH. I understand the question, and it ends—it extends well beyond a year, Senator.

The first step we took was the five services we mentioned to the Chairman a minute ago, which gets the consumer through 1 year. The ultimate control for security for a consumer is going to the lifetime lock, the ability for a consumer to lock down his or her file to determine who they want to have access for life.

Senator SASSE. But is not this—I would just interrupt. Is not this about people who might be breached in the future?

I am talking about the 145 million whose data has already been stolen. Does your responsibility end, or what do you think your legal obligations are to them?

Mr. SMITH. I think the combination of the five services we are offering combined with a lifetime lock is a good combination of services.

Senator SASSE. I actually think the innovation of some of the stuff you have proposed for the big three going forward is quite interesting, but why does any of that five really do much for the data that has already been stolen?

Mr. SMITH. Senator, again, the combination of the five offerings today plus the lifetime lock, we think is the best offering for the consumer.

Senator SASSE. OK. I do not think you have really answered the question about whether your exposure legally ends for the 145 million.

Do you know the number? Can you do the 145 million breakdown by State? Not off the top of your head, but do you have the data that we on the Committee could have by tomorrow? Just to—have you got it in your 145 million records? Can you parse it by State so each of us understands how many constituents we have——

Mr. SMITH. I believe so.

Senator SASSE. ——who have been exposed?

Mr. SMITH. We should have that capability. I am just hesitating on by tomorrow, but let me take that back to——

[Pause to confer.]

Mr. SMITH. We do have it.

Senator SASSE. OK. Great. Thank you.

It is being reported in the media this morning that you have just received a no-bid contract from the IRS for fraud prevention. Can you explain to the American people, not just as consumers who have been exposed and breached here, but as taxpayers, why in the world should you get a no-bid contract right now?

Mr. SMITH. I am not sure it was a no-bid. My understanding—I do not profess to have the details there, Senator—it is with the IRS. It is a contract we have had in the past. I think it is being renewed.

Senator SASSE. OK. We are going to follow up with the IRS as well, but if you could clarify back with us, my team will follow up with you.

I have less than a minute left, but I want to open at least the allegations that Equifax executives engaged in insider trading relating to knowledge of this cyberbreach. One of the clearest times and definitions of insider trading occurs when a business executive trades their company's stock because of confidential knowledge that they have gained from their job.

I am sure you can imagine why Americans are very mad about the possibility that this occurred here. Well, insider trading is going to be discussed a lot more later in this hearing. I wish you could just very quickly give us a timeline of the first steps. When did Equifax first learn of the May 2017 breach, and when did you inform the FBI of that breach?

Mr. SMITH. Thank you. I will answer as quickly as I can.

We notified the FBI cybersecurity forensic team and an outside global law firm on August 2nd. At that time, all we saw was suspicious activity. We had no indication, as I said in my oral testimony, of a breach at that time.

You might recall that the three individuals sold stock on August 1st and 2nd. We did not have an indication of a breach until mid to late August.

Senator SASSE. So you are saying that those three executives—Mr. Chairman, I will stop. You are saying those three executives had no knowledge of a breach on August 1st or 2nd?

Mr. SMITH. To the best of my knowledge, they had no knowledge, and they also followed our protocol to have their stock sales cleared through the proper channels, which is our general counsel.

Senator SASSE. We will have follow-ups on that, please.

Thanks.

Chairman CRAPO. Senator Tester.

Senator TESTER. Thank you, Mr. Chairman, and I want to thank you for being here today, Mr. Smith.

I apologize for not being here during your presentation. I had a business meeting on another committee, so I did not hear your timeline. So I will give you mine, and I will start with the first notification in March of this year by U.S.–CERT that you guys had a vulnerability. Did you do anything with that notification?

Mr. SMITH. Yes, Senator, we did. We were notified on March 8th and on March 9th, following the traditional patch protocol. Communication was sent out.

Senator TESTER. Communication was sent out. Did you do anything to fix the potential vulnerability?

Mr. SMITH. There were two steps that I discussed in my oral testimony——

Senator TESTER. Yeah. Go ahead.

Mr. SMITH. ——which I will walk through. One was there was a communication breakdown in the patching organization within IT. The message did not get to the right person down to the utilization of patch.

Senator TESTER. So, ultimately, nothing happened?

Mr. SMITH. Well, two things happened.

Senator TESTER. You did the notification, but ultimately, in the end, there was nothing done with that notification to fix that vulnerability?

Mr. SMITH. Senator, yes. A scan was applied looking for the vulnerability. A technology scan was applied, did not find it, so the patch was not applied. Correct.

Senator TESTER. OK. So let us fast forward to the 29th of July, and you learned for the first time that your company has been hacked, do not know how big the hack is, but it has been hacked, and it was preceded by this notification from U.S.–CERT.

Three days after, as Senator Sasse pointed out, you had three high-level execs sell $2 million in stock. That very same day, you notified the FBI of the breach. Can you tell me if your general counsel was held accountable for allowing this stock sale to go forward, or did he not know about the breach?

Mr. SMITH. Senator, a clarification. On the 29th and 30th, a security person saw suspicious activity, shut the portal down on the 30th. There was no indication of a breach at that time.

The internal forensics began on the 30th. On the 2nd, we brought in outside cyberexperts—forensic auditors, law firm, and the FBI. The trades took place on the 1st and the 2nd. At that time, the general counsel, who clears the stock sales, had no indication—or did the company—of a security breach.

Senator TESTER. Well, I am going to tell you something, and this is just a fact. And it may have been done with the best of intentions and no intent for insider trading, but this really stinks. I mean, it really smells really bad, and I guess smelling bad is not a crime.

But the bottom line here is that you had a hack that you found out about on the 29th. You did not know how severe it was. You told the FBI about the breach. On that same day, high-level execs sell $2 million worth of stock, and then you do some investigation, evidently, and you find out at the end of the month that—or at least by the first part of September that this is a huge hack, and you finally notify the public. And as was pointed out already in this Committee, these are people that did not ask for your service. You gathered it, and now it is totally breached.

And then, as Senator Sasse said, "What is the length of exposure here?" and you said, "Well, we are doing these five things." That is proactive, and I think we can all applaud those efforts. But I have got to tell you, that does not do a damn thing for the people who have been—had their identity stolen and their credit rating stolen.

So let me ask you this. So their credit rate goes up a little bit, and they go buy a house for 250,000 bucks on a 30-year note, and it cost them 25 grand. Are you liable for that?

Mr. SMITH. Senator, I understand your anger and your frustration. We apologize for the breach. We have done everything in our power to make it right for the consumer, and we think these services we are offering is a right first step.

Senator TESTER. Well, I would just tell you this, and I think Equifax must have—must be or been a good a company at one point in time, but this length of time on a breach this big in this day and age when we have folks that are pretty damn good at this stuff, especially when the Department of Homeland Security through U.S.–CERT says you got a problem, and was not really dealt with in a way like it was really a problem—I mean, you can

say you sent out the directives, but in the end, 3, 4 months later, you end up with a very severe breach.

The problem we have got here—and I will just tell you this—is that the impact and the numbers by State is important. I think it is about 600,000 adults, and I think it is about two-thirds of the adults in Montana, which is about probably 4 to 500,000 people, and in a State of a million, that is a lot, OK?

And so, consequently, those people are going to be impacted negatively for a long, long time. Why? Because this happened, and you can say, "Jeez, I am sorry it happened," but the notification for 6 weeks in this 21st century we live in is absolutely unacceptable. And I will just tell you that. It is unbelievable.

And I appreciate you coming in front of the Committee.

Chairman CRAPO. Senator Scott.

Senator SCOTT. Thank you, Mr. Chairman.

Mr. Smith, thank you for being here this morning, and certainly, we all are a tad confused about the knowledge that you had and your execs had that seem to—at least their stock sales seem to suggest more information than we are getting here.

So I just want to walk through the numbers as well as the timeline to better understand and appreciate what happened. You say that they did not know about the breach, but there was suspicious activity that was reported. Did you know about the suspicious activity on July the 29th?

Mr. SMITH. No, sir, I did not. So——

Senator SCOTT. You were not notified about the suspicious activity?

Mr. SMITH. I was but not on the 29th. So on the 29th, a——

Senator SCOTT. So the 31st, you were notified?

Mr. SMITH. Yes, correct.

Senator SCOTT. OK. So the very next day after you were notified, your senior executives, including your CFO, sold $1.8 million, nearly $2 million of stock, for a profit of—comparatively speaking to your September 7th devalued stock, for about $655,000. So at the price that the execs sold their stock for netted them, comparatively speaking, to the stock price that would have been on September 7th had they sold it on September 7th—they netted $655,000 during the same window that the average person who learned about the breach lost $6.4 billion or 36 percent of the stock value. Is that accurate?

Mr. SMITH. I have not done the math. I trust it is.

Senator SCOTT. OK. So Equifax tells the public about the breach on September the 7th, which is 6 weeks later, and just walk through the math with me, then. The stock dropped to $92.98 a share, and it dropped from $146.26 per share, or a 36 percent loss. The executives who sold the 1.8—1.8 trillion—$1.8 million benefited about $655,000 if you average in that 36 percent difference.

There are roughly 120 million outstanding shares of Equifax. That means that folks who have Equifax stock in their retirement accounts, the mom-and-pop businesses that are saving for the future for a large purchase and they decided to invest in Equifax, all those folks bore the burden of a $6.4 billion drop in valuation at the same time that the general counsel who did not know, the CEO who did not know, so all the folks in the executive suite had no

clue, but they were the luckiest investors on August the 1st to sell the stock at the best price to net $655,000. This was pure luck and nothing else. Question. Is it? Was it?

Mr. SMITH. No, sir. A few thoughts.

Senator SCOTT. Thank you.

Mr. SMITH. Go back to the 29th and 30th. We have—we experience millions of suspicious potential attacks each year. It is not like the suspicious attack that occurred on the 29th and the 30th was the first of that year, of that month. Suspicious attacks occur all the time. That is number one.

Number two——

Senator SCOTT. Let me ask you a question right there, sir. If you were to look back at the executives' stock sales on the other millions of suspicious activity, was there ever a suspicious activity that led to, within a 48-hour window, sale of stock?

Mr. SMITH. The window was open post the second quarter earnings call. It is only open for a short period of time, as you might guess. We encourage executives to sell the first part of that window's opening. As you get into the opening, you know more and more about the quarter and the financial performance of the company, so you tend to discourage sales later on in that month. So the behavior you saw was normal behavior. That is point number one.

Point number two is they did follow the protocol. They got the clearance. The general counsel approved the sale. The window was not closed by the general counsel until mid-August.

The last point I will make, Senator, if I may. These are three men I have known for a long time, two of them for 11 to 12 years. One has been my CFO for 3, 3½ years. These are honorable men who follow the protocol that was outlined by the organization.

Senator SCOTT. Well, I will just close with this, Mr. Ranking Member.

I believe in the rule of law for everyone. I believe that you are innocent until proven guilty, but I will say that what you guys want us to believe as a Committee, the U.S. Senate, the Congress, the investors in Equifax, and the entire Nation, what you all want us to believe is that the three luckiest investors who sold their stock did so without any knowledge that that suspicious activity may be bigger and more powerful than any other suspicious activity perhaps in the history of the company. I find that hard to believe.

Senator BROWN [presiding]. Senator Warner.

Senator WARNER. Thank you, Mr. Chairman.

Mr. Smith, appreciate you being here, but we have seen a history of other companies, of Yahoo! announcing today their breach was actually 3 billion, not the billion they initially acknowledged.

But for a company like yours, where American citizens have no right to opt in, we enter into no customer-based relationship with you, I think it raises a whole host of policy questions we cannot get into today, but I think this Committee needs to look at. I think we have to ask honest questions. Who owns this data? How do you get the right to this data that is our personal information, and yet your company's practices of cyberhygiene are sloppy in the extreme?

The fact that there was known vulnerability, that you did not have appropriate internal controls in place to easily patch this is inexcusable. The fact that it took so long for the senior leadership to get its act together is inexcusable, and what I find, what I want to spend my time, because I could echo what my colleagues have said about how long it took and everything else, but then once the breach was known, the complete, sloppy, haphazard approach you took on remediation is again inexcusable.

The fact that the site you put up, rather than you directed customers to go to, did not use your existing domain. You created a whole new domain site. In that domain site, there were known software glitches. You initially offered people what I believe was a bait-and-switch scam to say, "We are going to give you a year of free protection, but, oh, by the way, you are going to give up all of your legal rights by agreeing to some small-print arbitration agreement."

The fact that the site that you directed people to was so faulty and so sloppily put together, that even entities like the Architect for the Capitol would not allow users to access the site because they thought it was so vulnerable, the fact that you then also required individuals after their information had been hacked into, abused, potentially now vulnerable for who knows how long to enter in your last name and your last six digits of your Social Security number, what in heaven's name were you all thinking?

The fact that your official Twitter account mistakenly tweeted a phishing link four times instead of the company's actual breach response page, I mean, even if I want to try to give you the benefit of the doubt of sloppy cyberhygiene and somebody made a mistake and you did not find until after the fact and there were mistakes made, when this was all known and you said that you created a company that was an information-based company, you had this level of sloppy cyber-response? What do you say to the 143 million-plus Americans who have had their private information violated, that even after the fact, your response was inadequate and on every level would not meet basic cyber-101-hygiene standards?

Mr. SMITH. Senator, I understand your frustration and the anger of the American public. I apologize not only for the——

Senator WARNER. But, sir, I am not asking you to apologize. I am asking you to say how do we tell the American people. How should any American say again, "I have got no option of opting in whether you are going to get my personal credit information"? Why should any of us have any faith that you are putting anything in place that is appropriate when the immediate actions you took after the knowledge of the hack too place was so sloppy and so inadequate in terms of your remediation site?

Mr. SMITH. Again, Senator, the ramp-up was overwhelming for a company that is largely doing business with other companies, and we had to go from 500 call center people to almost 3,000 in 2 weeks. We went to the Cloud Computing Amazon site for scale. We had, I think I mentioned in my oral testimony, over 400 million consumers come to a website.

Senator WARNER. Sir, my time is up, but I would only say telling me how many more people you hired and scaled up, that is not what my question was. My question was, Why was your site so

technically flawed? Why did you send people to a new domain site that was not properly registered? Why was your Twitter account sending people to the wrong site? Why was this site so badly put together that institutions like the Architect of the Capitol would not even allow consumers to touch it because it was so faulty? For a company that claims to be an information-based company, even giving you the benefit of the doubt on everything that happened beforehand, your remediation efforts do not pass basic cyber-101-hygiene.

Thank you, Mr. Chairman.

Senator ROBERTS. Senator Perdue.

Senator PERDUE. Thank you, Ranking Member.

Thank you, Mr. Smith, for being here today.

Mr. Smith, just for the record, are you the current CEO of Equifax today?

Mr. SMITH. No, sir. I am retired.

Senator PERDUE. And you resigned your position; is that correct?

Mr. SMITH. Correct.

Senator PERDUE. Would you tell the Committee why you did that?

Mr. SMITH. Senator, I thought it was the best for the company to have a new leader come in and resurrect this great company. I have agreed, Senator, to work with the company for as long as needed. It has been a company I have loved working for, for 12 years. The company has done a lot of great things around the world. I have agreed to assist in any way I can for free for as long as they need.

Senator PERDUE. So, today, there are two issues before this Committee. I only have time in the few minutes here to get at one of these. The two issues are what happened, how did it happen, and what is going to be done to rectify that with the current individuals that were harmed by this.

The second issue is a bigger issue, and that is this entire cybersecurity issue. When the now Chairman Jay Clayton of the SEC was before this Committee, we asked this same question. Under the antitrust laws, there are limitations for corporations like yours and the other guys in this business to talk to each other when you are threatened by cyberattacks; is that correct?

Mr. SMITH. There are ways for us to talk to different entities when needed. The agency is an example. There is a network we belong to where we talk about issues and trends in cybersecurity. We take advantage of that.

Senator PERDUE. So in this situation, were you able to talk to your two biggest competitors when you were warned earlier in March and then when you discovered it in July?

Mr. SMITH. No, Senator.

Senator PERDUE. So why were you not able to talk to them and warn them of similar activity?

Mr. SMITH. I am not sure it was that we were not able to, but we did not know enough at that time either to talk to them.

Senator PERDUE. So later when you did know enough internally, were you limited by antitrust law or considerations, or were you able to fully talk to these other two competitors?

Mr. SMITH. That, I am not aware of.

Senator PERDUE. OK. We think there is a problem in that the Secretary—I mean the SEC Chairman is aware of that. Actually, Senator Cardin and Senator Blunt are working on a data security act that would provide a national standard and make it clear—because if you look at the current law, it is not clear—on these cyberbreach notifications for people within an industry and also between the companies and different agencies in the Federal Government.

A national standard like this, would that be helpful for your predecessor or your successors and other people in this industry?

Mr. SMITH. I believe so.

Chairman CRAPO. Let us talk about credit report freezes. It seems to me that in the day of the app, when my 6-year-old grandson knows how to get on and get unlimited access to apps, that a person who has data stored in one of these credit companies could go on an app that—and they are online right now, how to manage your credit scores and so forth. Intuit has got them. They are all out there. What keeps you from giving the ability to freeze an account?

Today, as I understand it, if you want to freeze your account, you have to go to your firm and each of the two biggest competitors and possibly others, pay a fee, get a PIN, remember the PIN, and then freeze it for—it is your determination, but to unfreeze it, you have to go back and activate the entire process again. That seems most Americans are not going to be able to do that.

So what keeps the industry from actually moving toward a simple app that some individual can be informed about to preclude this sort of exposure?

Mr. SMITH. Senator, that is a great question. That is where we are heading. That is the July—or the January 31st product or service that we are offering, which is—will be an application on a smartphone, on a PC. It allows you to freeze or lock and unlock instantly at the time you want.

I would encourage our two other competitors in the industry, Senator, to come together as an industry and offer that service to all consumers on one site. The things you could do if you had the consumers, the power at their fingertips, to lock and unlock anytime they want that for all three credit reporting agencies would be powerful. It would be a paradigm shift for the consumer.

Senator PERDUE. What would you tell your successor in terms of the number one—in most businesses, the number one entity they worry about is their customer. The individuals we are talking about, they really were not customers of Equifax. What advice would you give—and we have just got a few seconds left—what advice would you give your success to rectify this situation?

Mr. SMITH. Senator, we are a 118-year-old company. We have always prided ourselves as being a trusted steward of data. The number one thing we have got to do now as a company is regain the trust of the consumer in America.

Senator PERDUE. How do you do that?

Mr. SMITH. By doing what is right for the consumer. We are starting by doing, offering these five services, offering the lifetime lock. It takes time. When you have the size of criminal attack that we allowed to occur, it takes time to regain that trust.

Senator PERDUE. Thank you for being here.

Mr. SMITH. Thank you.

Senator PERDUE. Thank you, Mr. Ranking Member.

Senator ROBERTS. Senator Warren.

Senator WARREN. Thank you, Mr. Chairman.

Now, Mr. Smith, Equifax has been hacked several times in the past few years. It is consistently rated as having some of the worst data security practices in the financial services industry, and this latest hack happened through a hole in your system that had been identified months before and could have been fixed pretty easily. The whole thing is staggering. A company like Equifax that has sensitive personal information on most Americans should have the best data security in the industry, and instead, it has the worst. And I want to understand why.

So I started to look into this, and one thing jumped out at me. In August, just a couple of weeks before you disclosed this massive hack, you said—and I want to quote you here—"Fraud is a huge opportunity for us. It is a massive growing business for us."

Now, Mr. Smith, now that information for about 145 million Americans has been stolen, is fraud more likely now than before that hack?

Mr. SMITH. Yes, Senator, it is.

Senator WARREN. Yeah. So the breach of your system has actually created more business opportunities for you.

For example, millions of people have signed up for the credit monitoring service that you announced after the breach. Equifax is offering 1 year of free credit monitoring, but consumers who want to continue that protection after the first year will have to pay for it, will not they, Mr. Smith?

Mr. SMITH. Senator, the best thing a consumer could do is get the lifetime lock.

Senator WARREN. I am asking you the question. You are offering free credit monitoring, which you say is worth something, and you are offering it for only 1 year. If consumers want it for more than 1 year, they have to pay for it; is that right?

Mr. SMITH. Yes, Senator, but the most—the best thing a consumer can do is the lock product. That is better than monitoring.

Senator WARREN. OK. But they are going to have to pay after 1 year if they want your credit monitoring, and that could be a lot of money. So far, 7.5 million people have signed up for free credit monitoring through Equifax since the breach. If just 1 million of them buy just one more year of monitoring through Equifax at the standard rate of $17 a month, that is more than $200 million in revenue for Equifax because of this breach.

But there is more. LifeLock, another company that sells credit monitoring, has now seen a tenfold increase in enrollment since Equifax announced the breach. According to filings with the SEC, LifeLock purchases credit monitoring services from Equifax, and that means someone buys credit monitoring through LifeLock. LifeLock turns around and passes some of that revenue directly along to Equifax. Is that right, Mr. Smith?

Mr. SMITH. That is correct.

Senator WARREN. That is correct.

OK. So from the second Equifax announced this massive data breach, Equifax has been making money off consumers who purchased their credit monitoring through LifeLock.

Now, Equifax also sells products to businesses and Government agencies to help them stop fraud by potential identity thieves. Is that right, Mr. Smith?

Mr. SMITH. Yes, Senator. There is one clarification. You had mentioned the LifeLock relationship——

Senator WARREN. Uh-huh.

Mr. SMITH. ——which was accurate. At the same time, the majority of that revenue we normally generate is direct to consumer. We have shut that down. We are no longer selling a consumer product directly.

Senator WARREN. I am sorry. My question is every time somebody buys through LifeLock—and they have seen a tenfold increase since the breach—you make a little more money. We actually called the LifeLock people to find this out. So I asked you the question, but I already know the answer. It is true. You are making money off this.

So let me go to the third one. Equifax sells products to businesses and Government agencies to help them stop fraud by potential identity thieves, right?

Mr. SMITH. To the Government, yes, not to the business.

Senator WARREN. You do not sell the businesses, to small businesses?

Mr. SMITH. We sell to business, but it is not to prevent fraud. That is not the primary focus or business——

Senator WARREN. But to stop identity theft, you do not have any products that you are touting for identity theft purposes?

Mr. SMITH. Senator, all I am saying is the vast majority of what we do for businesses is not fraud.

Senator WARREN. Look, you have got three different ways that Equifax is making money, millions of dollars, off its own screw-up, and meanwhile, the potential costs to Equifax are shockingly low. Consumers can sue, but it turns out that the average recovery for data breaches is less than $2 per consumer, and Equifax has insurance that could cover some big chunk of any potential payment to consumers.

So I want to look at the big picture here. From 2013 until today, Equifax has disclosed at least four separate hacks in which it compromised sensitive personal data. In those 4 years, has Equifax's profit gone up? Mr. Smith.

Mr. SMITH. Yes, Senator.

Senator WARREN. Yes, it has gone up, right? In fact, it has gone up by more than 80 percent over that time.

You know, here is how I see this, Mr. Chairman. Equifax did a terrible job of protecting our data because they did not have a reason to care to protect our data. The incentives in this industry are completely out of whack. Because of this breach, consumers will spend the rest of their lives worrying about identity theft. Small banks and credit unions will have to pay to issue new credit cards. Businesses will lose money to thieves, but Equifax will be just fine. Heck, it could actually come out ahead.

Consumers are trapped. There is no competition, nowhere else for them to go. If we think Equifax does a lousy job protecting our data, we cannot take our data to someone else. Equifax and this whole industry should be completely transformed. Consumers—not you—consumers should decide who gets access to their own data.

And when companies like Equifax mess up, senior executives like you should be held personally accountable, and the company should pay mandatory and severe financial penalties for every consumer record that is stolen.

Mr. Chairman, we have got to change this industry before more people are injured.

Thank you.

Chairman CRAPO [presiding]. Senator Tillis.

Senator TILLIS. Thank you, Mr. Chair.

Mr. Smith, thank you for being here.

I have one question that I want to get to. First, can you explain to me why you believe as a strategy the lock versus the delete option is in the best interest of the consumer?

Mr. SMITH. Yes. Senator, we, I think, provide a very valuable service to the consumer, allowing he or she to get access to credit when they want access to credit. If they are not in the system, they hinder their ability to get credit.

Senator TILLIS. How do you think that would—let us say that you had a delete option, so there was not a transactional opportunity for a consumer to have that information available to people who are maybe underwriting a loan. Let us say that if you took that to the logical conclusion and had all three of the information providers delete your financial record, how do you think that would affect somebody who is trying to apply for a mortgage or a loan or a credit card?

Mr. SMITH. We know what would happen. If you are not in the credit ecosystem, you do not get a loan.

Senator TILLIS. Do you think that is maybe even particularly more pronounced, given some of the changes that we have with financial regulations and underwriting practices and scrutiny from the Federal Government?

Mr. SMITH. I do.

Senator TILLIS. Look, the point that I am trying to make here is you all have a problem. I associate myself with a lot of the concerns.

One thing I would ask you to do, you said the three individuals in question for a stock disposition are honorable people, that you have known them for several years. They have been employed by Equifax for several years. I think it would be very helpful to see what their pattern of stock dispositions have been over the years to see the process they have gone through, because I think that that would be helpful for this Committee. I think there is an appearance issue there that you all should—or that Equifax and the individuals should step up and address.

Look, here is the other thing that we could be missing here. You all made a big mistake. You sound like you have got some remediation practices in place. I think you do have to get right on the long-term obligation you may have. There is a difference between a breach and exploitation.

At least the other day, when I asked about any evidence of exploitation of the data breach, we have not seen any yet, but it seems to me, you have got to create some sort of a footprint on the data that was exploited so that over time, you could make a reasonable decision about whose problem it is to remediate any exploitation beyond the year pathway.

Another thing—I mentioned it yesterday with Wells Fargo—that I think is very important, the problem that resulted for maybe controls and processes at Equifax should be your problem, not the consumer's problem. In other words, you need to make it very easy and no cost to the consumer to fix a problem that they became a part of, and rather than you get into the details in this Committee, it would be helpful for me to get some assurances that that is the case.

I use an example of an inappropriate parking ticket that I got using a park mobile app in Charlotte. When I called the folks up and said, "I got a receipt right here," they said, "Well, you can go through 2 or 3 weeks. You can appeal. You can file it, and we are sure that it was because maybe your license tag got mixed up." I said, "My license tag at the time was a 3." So I think they should have been able to figure it out, but they were trying to make their problem my problem. And you need to be absolutely certain—or Equifax and the people that are taking the helm need to be absolutely certain that they can convince us that you are addressing this and not making your problem the consumer's problem.

I do think it is very important for people to understand the potential chilling effect that you could have if you erase your financial history from the system. We expect you all to protect it, and we expect you all to be good stewards of it. In this case, a variety of factors led to that not being the case, but we have to get there.

I had another—just a comment to make. You are an aggregator of data. What this Committee and every committee that is taking a look at for cybersecurity needs to understand, the broad exposure that we have in this country. You are an aggregator of data. Again, I would think that your systems should be more impervious to attacks than mom-and-pop shops and other people who are aggregators of data based on their purchasing platforms and their supply chains.

Congress needs to start thinking big picture here and how we can get the U.S. economy to a point to where when you become difficult or more difficult to penetrate, then I just go to the sources. And then I can pick it off and maybe actually do it in organizations that are far less sophisticated than you.

If people think that the credit reporting agencies and the big banks are the only ones that are vulnerable, I would suggest that you go get a book that I have got on my desk right now in my office. It is called "Hacking for Dummies". It is a very important book for you all to understand, for the industry to understand, and for Congress to understand.

You need to be held accountable. Equifax needs to be held accountable. We need to be held accountable for actually getting beyond the shiny objects of this breach, which are really important, and you need to protect the consumers and recognize we have a role to play to protect this economy, otherwise this is not going to

end. It will be the CEO of the week and the breach of the week, and that is not the way that we should be leading from Capitol Hill.

Thank you for being here, and we will potentially submit some other questions for the record. But I think it is in your best interest or those who are working with Equifax to give us more information on the stock disposition patterns for the executives in question.

Thank you very much.

Mr. SMITH. Thank you. I understand, Senator.

Chairman CRAPO. Senator Heitkamp.

Senator HEITKAMP. Thank you, Mr. Chairman.

North Dakota is a State of about 740,000 people. Our Attorney General estimates that 248,000 North Dakota families have been affected by this, and let me tell you, I have heard from a lot of them. And I want to just tell you that I am deeply concerned about the remedial efforts and how all of that rolled out to begin with.

First off, if you have this level of information on consumers that they did not give you—that is all part of this thing that Elizabeth was talking about—and you do not have a system in place for a fire drill on what you do if you are breached, after you told us that you get notifications all the time of potential breaches—and then you say, "Oh, we had to create all of this system. We had to create this thing out of whole cloth," right? That is what you have told us—why the roll-out after the breach was notified, why it went so poorly, and why people were not protected, and why in many cases, it was like, "OK. We are going to charge you a fee if you do this. We are going to do this," my consumers are like, "Why do I have to now spend money to protect myself when it is their fault?"

And so I think it is not enough for you to say, "My goodness, look at the magnitude of this," when you should have anticipated it, the same way you should anticipate whether you have a fire in a building. You should be ready when it happens, and it goes to what Senator Tillis just said. We all know it is going to happen again, and I am saying this because I want all CEOs who have access to this kind of information to know I am going to ask a question on what they are doing to prepare, to prepare for a breach.

Now I want to get back to the FBI. You said, "Look, we get a lot of these breaches. You know, this happens all the time. We did not realize it was as serious as what it was." What is the date you notified the FBI, and who made that notification?

Mr. SMITH. Senator, the date was August 2nd. The head of security at that time would have notified the FBI, the cybersecurity forensic team, and King & Spalding.

Senator HEITKAMP. And when would the head of security have notified your chief legal counsel or chief legal officer?

Mr. SMITH. On and around that same time.

Senator HEITKAMP. Yeah. And when did he approve the stock trades?

Mr. SMITH. Senator, he approved the stock trades on the 1st and the 2nd for the three individuals. At that time, as I alluded to earlier, it was a suspicious activity. There was no indication of a breach at that time.

Senator HEITKAMP. How many times do you notify the FBI? You do that every day, every week?

Mr. SMITH. I do not have that specific data, but it is not unusual. I mentioned earlier that we have millions——

Senator HEITKAMP. I get that. I want to know how many times when you are notified, you actually turned around and notified the FBI.

Mr. SMITH. We can get that information. I do not have that.

Senator HEITKAMP. Yeah. Well, that is a problem because it looks pretty suspicious, and your chief legal officer has some explaining to do because even after he knew that there was a notification to the FBI about this level of breach, he did not clawback or try to undo those transactions and reverse what clearly appears to be a pretty beneficial situation for three of your employees.

I want to talk about remedial measures and go back to consumers. Obviously, we are in this very big discussion about what we are going to do with mandatory forced arbitration.

You know, it is interesting because if I go out there and sign a contract with somebody, maybe I can protect myself. Maybe I cannot. I do not think that fine print in a contract is exactly anything other than illusory, but we can argue that point. But why should you ever make that choice and mandate forced arbitration in your business?

Mr. SMITH. Senator, a point of clarification—and this is part of our—my apology earlier—the intent was never to have arbitration clause in the product that—the services offered to the consumer at that time. It was a part of a boilerplate. It was a part of a product we were offering to consumers prior to the breach. It was a mistake we made.

Senator HEITKAMP. But let us just ignore for a minute the breach. Why should the consumer not be able to make that choice, especially in this situation when the consumer is not your community?

Mr. SMITH. Again, to be clear, that was not the intent for the breach. Arbitration clause is a legally, viable path for us to take at this time. That is why it was in the consumer offering.

Senator HEITKAMP. Yeah. Well, I think we have got some real challenges in taking a look at how we provide a real remedy to consumers in this situation, and this will not be the first time that we have a hearing like this. We had one yesterday; we are having one today.

But I guess my warning, Mr. Chairman, would be I am going to ask every person out there who has responsibility as a CEO for consumer data to do the right thing, and that is right now start thinking about if this happens to me, how do I treat my consumers and the people who have lost their personal data. And maybe we ought to start thinking about opting in as opposed to opting out.

And so I want my credit locked until I do not—until I unlock it. Why cannot I have that option? Why do I have to pay to have my credit locked?

Mr. SMITH. Senator, you do not. It is free. It is part of the offering we just made.

Senator HEITKAMP. For the breach, yeah.

Mr. SMITH. For lifetime.

Chairman CRAPO. Senator Schatz.

Senator SCHATZ. Thank you, Mr. Chairman.

You are retired as of last week. You leave with your base salary, unvested options, and a pension, roughly valued at $90 million. Help me to understand why that is fair.

Mr. SMITH. Those numbers do not resonate with me, Senator.

Senator SCHATZ. Well, what is the number, then? You should know.

Mr. SMITH. Clarification. I stepped down last week. I told the board at the time I stepped down, I will not take a bonus. There is on severance. I will work for as long as the company needs for free. I have asked for nothing. What I walk away with is a pension that I have earned over my career and unvested equity that was given to me and I earned in the past.

Senator SCHATZ. Is it fair to say that is in the tens of millions of dollars?

Mr. SMITH. It is in the proxy. The proxy discloses the value of the——

Senator SCHATZ. Right. And that is how we got to $90 million, but if it is $45 million or it is $23 million or it is $38 million, my question stands. How is that fair?

Mr. SMITH. The pension, Senator, is something I have earned for my career, and the other piece is the earned equity I have already been given.

Senator SCHATZ. Do you think that is fair?

Mr. SMITH. Senator, I grew up as a young guy in Midwest. I never envisioned having a career like I have had for the last 36 years. I have been fortunate. I have worked hard, and I do not set those compensation levels. The board does, and the board is elected every year.

Senator SCHATZ. Your investor presentation from August 16th, 2017, mentions nothing about the data breach, even though by July 29th, you knew that your system had been compromised. By August 2nd, you had retained outside counsel and informed the FBI. I understand that you periodically inform the FBI. I assume you do not necessarily consistently retain outside counsel. I assume at some point around August 2nd, you knew that something more significant than usual was up; is that true?

Mr. SMITH. No, that is not true, Senator.

It was not until later in August that we had some indication, the size, the scope, and the complexity of the breach. It was not on August 2nd.

Senator SCHATZ. So August 16th, your message to investors was, quote, "Enduring business fundamentals support long-term growth," and the first time data security is mentioned is at the end of your materials where you tout your role as a trusted steward of consumers' data. Do you think that Equifax should have disclosed the possibility of a major data breach to its investors?

Mr. SMITH. Senator, we talk to investors routinely. We disclose in our 10-K and Q's that one of the greatest risks we pose each and every day and fight every day is cybersecurity.

Senator SCHATZ. Right. But you retained outside counsel. You informed the FBI. People are liquidating their stock, and I guess I am wondering whether that pattern seems to indicate that somebody knew something pretty significant was up. But somebody made a judgment to not disclose that, not just to 143 million Amer-

icans but also investors. It seems to me that that is material. It seems to me that that is reportable, and whether or not you follow the letter of the law, it seems to me that investors ought to know if something is going to impact the company. And you had to have some clue that this was percolating in a negative way.

Mr. SMITH. Senator, we are very transparent with our investors that security is always a risk. They are very well aware of that. They price that into their value of the company.

Obviously, on the 16th, I think, is what you refer to, the investor relations team had a presentation, on or around the 16th. We had not gone public with anything. We did not know the scope or the size of a breach, so obviously, we could not disclose that at the investor meeting.

Senator SCHATZ. Right. So you did not know the total scope and size of the breach. I get that. So you decided not to disclose it at all?

Mr. SMITH. To the investors?

Senator SCHATZ. Yes.

Mr. SMITH. Yes. Because at that time, we were even uncertain if there was a breach at that time, and you could not go to an investor base and tell an investor base something before we had gone public with something.

Senator SCHATZ. And why would not you inform the public about it?

Mr. SMITH. Sir, the timeline, as I walk through, from the 28th, 29th, and 30th of July through September 7th lays that out, and it was not until late August we actually had an indication of the breach.

Senator SCHATZ. So what happened on July 29th?

Mr. SMITH. July 29th is when a security individual saw suspicious activity, on the 30th saw it again, shut down the portal to stop the incident.

Senator SCHATZ. And then it took you 6 weeks to figure it all out?

Mr. SMITH. Yes. Again, we bring in the cybersecurity experts who do this for a living, and the complexity, the size, the movement——

Senator SCHATZ. You do not do it very well for a living, except to the extent that you make massive profits off of making mistakes. I understand you do this for a living, but to the extent that none of us have the volition to enter into a contract with you, you are not doing it well for a living, except that you are all making a very nice living at it.

Thank you, Mr. Chairman.

Senator BROWN [presiding]. Thank you, Senator Schatz.

Before calling Senator Kennedy, I want to do a clarification. Senator Sasse asked about if you had State-by-State information. You seemed unsure. Your team informed you in real time that, in fact, you did have that.

Chairman Crapo and I had sent a letter September 22nd requesting that State-level data on victims, so it appears that your team has this information. Why was it not provided to us in response to our September 22nd letter to the Chairman and me, the State-by-State data?

[Pause to confer.]

Mr. SMITH. I was just informed by Senator Chambliss that it was given to each of the State AGs earlier. There are, as you saw, a released by the company—I believe it was Monday—of another 2.5 million consumers impacted. That has not yet been distributed to the AGs. I am told the AGs, State AGs have that record.

Senator BROWN. OK. We are not the State AGs, and the Chairman of the Banking Committee and the Ranking Member cosigned a letter. We do a lot of things bipartisanly in this Committee, and that letter was sent—it looks like 2 full weeks ago, and it was not provided, so I hope that you will get that to us quickly. And that is not the way that you should operate.

Senator Kennedy.

Senator KENNEDY. Thank you, Mr. Chairman.

Thank you for being here. I am over here, Mr. Smith.

I found out about Equifax's contract with the Internal Revenue Service in an interview this morning with Stuart Varney. How big is that contract?

Mr. SMITH. Senator, I saw it this morning as well. Maybe it was last night, and it referenced a $7.5 million contract. I am not sure if that is multiyear.

Senator KENNEDY. Do you have other contracts with the Internal Revenue Service?

Mr. SMITH. We may, sir, but I am not aware of it.

Senator KENNEDY. Could you get me a list of all of Equifax's contracts with various Governments?

Mr. SMITH. Yes, Senator, we can do that.

Senator KENNEDY. The contract, the 7-million-and-change contract, does that involve taxpayer information that you would have access to?

Mr. SMITH. Senator, it is my understanding—I am not professed to be deep in this particular contract—it is to prevent fraudulent access to the IRS, but beyond that, I—if you want more information, we can get that for you.

Senator KENNEDY. Well, you realize to many Americans right now, that looks like we are giving Lindsay Lohan the keys to the mini bar.

Mr. SMITH. I understand your point.

Senator KENNEDY. Let me ask you about a credit freeze. I went through that. I have frozen my credit at all four of the bureaus. I would like a commitment from you today that you are going to ask your former company, though I think you still own quite a few shares—I want you to make a commitment to putting a free app available to anybody so that you can just go to your app, toggle on and off, access to your credit files.

Mr. SMITH. Senator, I agree with you. We like that idea. That is going to go live for every American consumer the end of January 2018. That will be free for life.

Senator KENNEDY. So you are committing to do it?

Mr. SMITH. Yes. Senator, we have been working on that for months.

Senator KENNEDY. OK. This whole unfortunate experience, Mr. Smith, has raised larger issues, and one of the issues that it has raised is to whom does your former company—I will call it your

current company because you are still working there. To whom does your company have an obligation?

My understanding of your business model is that you collect my information without my permission. You get the information. You take it along with everyone else's information, and you sell that information to businesses. Is that basically correct?

Mr. SMITH. That is largely correct.

Senator KENNEDY. And you also have a premium service to monitor the information that you collect about me. So if there is some bad information that you collect about me, you sell me a service to monitor it and correct it; is that right?

Mr. SMITH. Senator, just a clarification. Roughly 90 percent of everything we do is helping banks and others make informed decisions about lending money to consumers. The monitoring you are referring to, to consumers, is a very small piece of what we do.

Senator KENNEDY. But it just seems incongruent to me that you have my information. You do not pay me for it. You do not have my permission. You make money collecting that information, selling it to businesses, and I think you do a service there. Do not misunderstand me.

And you also come to me—you cannot run your business without me. My data is the product that you sell, and you also offer me a premium service to make sure that the data you are collecting about me is accurate. I mean, I do not pay extra in a restaurant to prevent the waiter from spitting in my food. You understand my concern?

Mr. SMITH. I understand your point, I believe, but another way to think about that is the monitoring part that you are referring to, Senator, in the future is far less required if you as a consumer have the ability to freeze or lock, as we call it, and unlock your file. And that is free for life.

Senator KENNEDY. But it is not just the freeze part. What if you have bad information about me? Have you ever—has an agency ever had bad information about you, and you had to go through the process of correcting it?

Mr. SMITH. Yes, Senator. There is a process that if——

Senator KENNEDY. It is a pain in the elbow, isn't it? I mean, the burden is kind of on—you have my data, which you have not paid me for. You are earning a good living, which I do not deny you. I believe in free enterprise. I think this is a very clever business model you have come up with, but you are earning your money by selling my data, which you get from me and do not pay me for, to other people. But if the data is wrong that you have about me, I would think you would want to make it as easy as possible to correct it, not as hard as possible.

Mr. SMITH. I understand your point, and it is an important point for the entire industry to make the process as consumer-friendly as possible. If there is an error on your utility bill, if there is an error on your bank bill, your credit card statement, to work with consumers and make that——

Senator KENNEDY. Well, can you commit to me today that Equifax is going to set up a system where a consumer who believes that Equifax has bad information about him can pick up the phone and call a live human being with a beating heart and say, "Here

is this information you have about me that you are selling to other people. You are ruining my credit, and it is not true. And I want to get it corrected. How are you going to correct it? What information do you need from me to prove that it is incorrect, and when are you going to get back to me? And give me your name and phone number so I can call you"?

Mr. SMITH. Senator, I understand your point. There is a process that exists today. I would be more than happy——

Senator KENNEDY. Yeah. And it is difficult, Mr. Smith.

Mr. SMITH. I would be more than happy to get the company to reach out to your staff, explain what we do and what we are doing to improve that process. I hear you.

Senator BROWN. OK. I thank you, Senator Kennedy.

Senator KENNEDY. I am sorry. I went way over. I apologize.

Senator BROWN. That is all right.

Senator DONNELLY. Thank you, Mr. Chairman.

Mr. Smith, on September 19th, myself, Senator Heller, Senator Tester, Senator Menendez sent you a letter, and the letter we sent expressed concerns about the impact on the roughly 1.3 million active duty U.S. military personnel, especially the nearly 200,000 currently stationed overseas who may lack the access and resources required to place a credit freeze on their files or take other necessary measures to adequate protect their personal information.

We requested you immediately detail the specific actions Equifax will take to ensure our servicemembers are not victimized any further by thieves with access to personal information, such as Social Security numbers, dates of birth, and home addresses.

In response, I received a generic letter from Equifax that never even mentioned servicemembers, that basically said thank you for your interest.

In your written testimony today, you also make no mention of our servicemembers or the military. So I will again ask a question that should have been answered: What specific actions will Equifax take to ensure our servicemembers are not victimized any further?

Mr. SMITH. Senator, let me apologize if we did not get back to you. That was—someone dropped the ball, and I will look into that quickly for you.

The servicemembers around the world have the same ability, if they have access to the Internet, to freeze, lock, get access to products. If not, they have the ability to have a power of attorney in the U.S. to act on their behalf.

Senator DONNELLY. Well, let me ask you about some of our young men and women who are at forward operating bases in Iraq or in Afghanistan, who may be somewhat other occupied——

Mr. SMITH. Yeah.

Senator DONNELLY. ——than having the chance to get on the computer and get their lock going on. So let me ask again and say for those members who are serving in remote or high-conflict areas, what is it that you can do to make sure that their identities and financial information are safe?

Mr. SMITH. Again, they have the ability to have a power of attorney, and that power of attorney can act on their behalf.

Senator DONNELLY. You know, that is pretty weak tea for someone who is in a location where they may be occupied keeping our country safe and having their hands full with others.

Mr. SMITH. Senator, let me take that on. I will get back with the company and see if there is anything else we can do specifically for those overseas.

Senator DONNELLY. Let me ask you another question. Due to the cyberattack, roughly 145 million Americans have had their information compromised, and Equifax has said you now offer free credit freeze. But there is also Experian and TransUnion, and what I want to know is, Will Equifax also offer free credit freezes at Experian and TransUnion to ensure consumers are protected from theft and fraud?

Mr. SMITH. Senator, the lock that we offer for free for life is a product that I believe the entire industry should rally around. It is my understanding that TransUnion, one of the two other credit reporting agencies, also offers a lock product for free. It is my understanding it is not for life at this time, but they offer it for free.

Senator DONNELLY. Well, this breach was caused by Equifax. What will Equifax do to ensure that there are free credit freezes for those 145 million Americans at Experian and TransUnion as well? I do not want to see folks have to rally around this or rally around that or try to figure out how to navigate the Internet to get it done for themselves. What will you do for those 145 million Americans, our friends and neighbors, millions in my State, that will provide a free credit freeze at Experian and TransUnion?

Mr. SMITH. Again, Senator, the things we have done is the five services we offered for 1 year combined with a lock for life—and I would invite TransUnion and Experian to follow suit——

Senator DONNELLY. But those services you just described do not include a free credit freeze at Experian and TransUnion.

Mr. SMITH. That is correct.

Senator DONNELLY. So, in other words, Equifax will not do anything to provide that?

Mr. SMITH. Again, we are offering our five services plus lock of life.

Senator DONNELLY. Well, I guess that answers the question that I was asking, which then leads to my next question which is, What is Equifax's obligation to consumers who fall victim to identity theft or financial fraud in the future due to this breach? The damage caused to their credit, the money they may lose, how does Equifax plan to address the financial harm that can come to our families?

Mr. SMITH. Senator, the design, the thought was offer these five services, allow someone to lock their file for life to minimize the downstream harm.

Senator DONNELLY. But what happens if someone is harmed?

Mr. SMITH. Senator, that is the extent of our offering.

Senator DONNELLY. So because of your failure to stop this breach and a family is damaged financially, there will be no compensation provided?

Mr. SMITH. Again, Senator, the five services we are offering are for free. The lifetime lock is for free.

Senator DONNELLY. Which does not touch at all upon the question I just asked.

Thank you, Mr. Chairman.

Chairman CRAPO [presiding]. Senator Rounds.

Senator ROUNDS. Thank you, Mr. Chairman.

Mr. Smith, I would like to go back into a little bit different question for a little while. I would suspect that there are probably thousands of CEOs and board chairmen for publicly traded companies as well as some large private companies that when they heard about the theft of data that was in your care, custody, and control, that they looked back at their own operations and said, "Can that happen to us?" And I would suspect that there were a number of chief information officers out there who were being called into the front offices to explain and to reassure that they did not have the same vulnerabilities that were found within your operation.

I also suspect that since you have got experience in working in multiple major organizations that you have seen how boards work and that you have seen how the bosses do their own type of a command and control and get feedback.

I would imagine that you have lost a lot of sleep wondering what it was that you could have done differently and what message you would send to other individuals if given the opportunity.

We are going to have a lot of people that get hurt on this, and they are people that you had data from. If you could go back a year and look at your operation and tell us what you would do differently to demand things be changed, if there was any inkling at all, what would you do?

Mr. SMITH. Senator, as you might guess, since early August, myself and the entire team that has been focusing on addressing this issue has been working around the clock trying to, first and foremost, understand the forensic of what occurred and maybe why it occurred and then communicating to consumers and regulators and State AGs and the like. I have had no time to reflect on, as a leader who has apologized and takes full responsibility, what I would do differently. I am sure when I have time to reflect, there will be things I look back on and say, "If I only had done this." That time will come, but, Senator, to be honest, I have not had that time to reflect.

Senator ROUNDS. As many board members or chairmen would do, they rely on a CIO to provide them with assurances. Did you as a member or with the board doing their due diligence—do you feel that the due diligence that was expected of you as a board and as the chief operating—or the chief executive officer—do you feel like you did the due diligence necessary to assure yourselves and to get second opinions, that the CIO was actually doing the job that they needed to do, and that they were doing their own sense of due diligence in this process?

Mr. SMITH. The CIO I had has been there for 8 years. He was a very seasoned CIO. Ultimately, the responsibility stops with me, not him. He is no longer with the company nor is the chief security officer, but ultimately, that responsibility stops with me, Senator.

Senator ROUNDS. I read your article. I read through your statement, your written statement, and I caught time and again—and we sometimes—we go for the fact that you were the victim of theft

as well. There were bad people that got into your system. The obligation that you had to protect that information that was in your care, custody, and control is clear. And I think that sometimes organizations that have that data, they assume that somebody else is doing their job. They assume that there are reasonable expectations of due diligence being completed.

I guess what I was hoping to hear is something along the lines of "Yeah. If I could send a message to other CEOs out there, it is do not just listen. Do the double-checks. Find out. Ask for the outside assistance," and I guess I am not hearing that. And I know that this is early in your process, but nonetheless, it seems like that would have been one of the first things that most CEOs would have said is "If I could do this over again, I would have fixed this. I could have had an opportunity. Why did not I think of it?" I just—I am looking for that.

And I know that you did make a point in there saying, "We are using Social Security numbers out there, and we have got to go to a different system." If nothing else, you have thought about that. What would you do or what would you recommend in terms of a different system for identifying and maintaining data that belongs to individuals safe in a case like this? What can we do different?

Mr. SMITH. Yeah. I do not have that answer. I have spent a lot of time talking to people in the cyberworld, and they are convinced—they have convinced me that there has to be a better solution than an instrument that was introduced in 1936. It was never intended as an identifier for an individual.

I am convinced that if you get the public, private, and academic partnership, we can crack that.

Senator ROUNDS. But no real answer yet?

Mr. SMITH. Not yet.

Senator ROUNDS. Thank you.

Thank you, Mr. Chairman.

Chairman CRAPO. Senator Van Hollen.

Senator VAN HOLLEN. Thank you, Mr. Chairman.

Mr. Smith, it is good to have you here. Consumers do not authorize Equifax or any credit reporting agency to collect their personal information, do they?

Mr. SMITH. Not to collect it.

Senator VAN HOLLEN. No. So you vacuum up lots of information, and you provide it to people who say they are interested in the credit of somebody who may be applying for a car loan or a home loan or other loan, right?

Mr. SMITH. Yes.

Senator VAN HOLLEN. So you have an incredible amount of power over people's lives, right? You collect all their personal information, and yet their life decisions may, in many cases, depend on what you say to a bank or another lender. Is not that right? OK. Is not it a fact that when someone goes for a loan, if you tell a lender that someone is a bad risk, they are a lot less likely to lend?

Mr. SMITH. Senator, I thought that is where you were going. We do not make that delineation for the bank. We have that data, may provide some analytics behind it, but ultimately, the banks——

Senator VAN HOLLEN. But you provide the credit scoring, right?

Mr. SMITH. There is an individual firm called FICO that provides the score.

Senator VAN HOLLEN. And they do that based on the information you provide, right?

Mr. SMITH. Correct.

Senator VAN HOLLEN. OK. Now, are you aware of the fact that when the Consumer Financial Protection Bureau did a survey, they found that Equifax, Experian, and TransUnion are the three most complained-about companies in America? Are you familiar with that finding?

Mr. SMITH. Yes. It is a little misleading.

Senator VAN HOLLEN. Well——

Mr. SMITH. That is the CFPB Complaint Portal. If I may, Senator?

Senator VAN HOLLEN. Well, no. Unfortunately, if the Chairman wants to give me more time, I will, but I will—I will just—you can submit something for the record, if you are interested, but I think the point I wanted to make is this was actually from September 8, 2016. I mean, this is even before we had the incredible introductions into the data and the exposure of data.

People pay many other companies billions of dollars in the event that you make a mistake that needs to be corrected. Is not that the case?

Mr. SMITH. I am sorry. State that again?

Senator VAN HOLLEN. People, consumers who have information incorrectly included on one of your reports, they often have to pay a lot of money to other firms to get it corrected. Is not that the case?

Mr. SMITH. No, that is not the case. If a consumer has a—you referred to in the CFPB——

Senator VAN HOLLEN. I am talking about the credit repair services. What do they do?

Mr. SMITH. Yeah, but the process the consumer could use, if they think they——

Senator VAN HOLLEN. No, but what about—what—the credit—I am asking these credit repair service companies—they are making money now to try to help consumers correct mistakes that are often put in your reports or other credit rating agencies. Is not that the case?

Mr. SMITH. There is an industry that does that, Senator. A consumer can come to us directly and dispute that issue.

Senator VAN HOLLEN. So I guess those industries are making billions of dollars, but they really do not need to exist, in your testimony. All they have to do is come to you.

Are you aware of the fact that—I just—Mr. Chairman, I would like to put in the record, a *Washington Post* story from 2008—16, how the careless errors of credit reporting agencies are ruining people's lives.

Chairman CRAPO. Without objection.

Senator VAN HOLLEN. I would also like to include in the record something from CNBC, a piece by Aaron Klein, a fellow at the Brookings Institute, titled "The Real Problem With Credit Reports Is the Astounding Number of Errors".

Chairman CRAPO. Without objection.

Senator VAN HOLLEN. And I would also, Mr. Chairman, like to put in the report the FTC study from February 2013 that said 5 percent of consumers had errors on their credit reports that could result in less favorable terms for loans.

Chairman CRAPO. Without objection.

Senator VAN HOLLEN. Because the whole model of this industry is you collect information without permission from consumers, and yet their lives depend, in many ways—their economic lives depend on decisions you make.

So I want to go back to something Senator Heitkamp asked you with respect to forced arbitration because, clearly, we have a powerful company that is often up against one individual who is trying to get something corrected on their credit rating report or whatever it may be, and yet in the aftermath of this incredible breach, you said that you would provide credit protection but only if consumers gave up their right to get their day in court. You want to have forced arbitration.

Now, your testimony today is that was a mistake, that you did not mean to apply it in this case; is that right?

Mr. SMITH. That is correct.

Senator VAN HOLLEN. All right. But you do apply forced arbitration in many other situations, don't you?

Mr. SMITH. In the consumer products.

Senator VAN HOLLEN. And so if you are looking out for the rights of consumers, why do not you give them the choice of how they seek their remedy?

Mr. SMITH. Senator, I understand your issue today. That arbitration clause is a legal provision, and we follow that.

Senator VAN HOLLEN. And you have been—not just legal, but you have paid lobbyists on Capitol Hill—I am asking you a question, then. Have you paid lobbyists on Capitol Hill to fight the rule that was put forward by the Consumer Financial Protection Bureau?

Mr. SMITH. If you are referring to the harmonization bill that was proposed, which I think you are referring to—is that the bill?

Senator VAN HOLLEN. I am referring to the legislation——

Mr. SMITH. Arbitration specifically?

Senator VAN HOLLEN. ——that would overturn the Consumer Financial Protection Bureau's rule that prohibits forced arbitration clauses.

Mr. SMITH. Senator, if we spent time on that, I am not aware of that.

Senator VAN HOLLEN. So are you in favor, then? You said it is part of the law, and so you are just abiding by the law. But as somebody who has experience in this area, would you agree that consumers should have the right to decide how best to protect themselves in legal matters?

Mr. SMITH. Senator, if that becomes law, we will follow the law.

Senator VAN HOLLEN. No, that is not my question.

Mr. SMITH. I understand.

Senator VAN HOLLEN. My question is, Where do you stand on the issue of allowing consumers to choose how they seek recourses when they believe they have been wronged?

Mr. SMITH. Senator, I understand the question, and today, arbitration is a part of the law, and we are following the law.

Senator VAN HOLLEN. Yeah. And so you are following it even though it may be unfairly treating consumers; is that right?

Mr. SMITH. I understand your question.

Senator VAN HOLLEN. But, Mr. Chairman, if I just—but you chose to suspend that law. You could have enforced that on these individuals, right?

Mr. SMITH. It was never the intent, as it related to the breach——

Senator VAN HOLLEN. But it was the law. The law would have allowed you to do it, right?

Mr. SMITH. But it was never the intent——

Senator VAN HOLLEN. That is not what I am asking. The law would have allowed you to do that, right?

Mr. SMITH. Yes.

Senator VAN HOLLEN. And you chose not to because you thought in that circumstances, consumers would be better protected by having choices, and my only question to you, if it is good in that circumstances, why is not it good for consumers all the time?

Thank you, Mr. Chairman.

Chairman CRAPO. Thank you.

Now, that concludes the questioning, however, we have had a couple of requests for a second round, and so I will go with a brief 3-minute second round.

Senator.

Senator BROWN. Thank you, Mr. Chairman.

Following up on, I thought, Senator Van Hollen's very good line of questioning about your rather curious statement that you are following the law, but you are not following the law on the—in the one case, but you are in the other, I do not entirely get that.

But let me take it a different way. In your written testimony, you state that terms and conditions attached to the free solutions that Equifax offered included an arbitration clause. You said this provision of forced arbitration clause was never, in this case, intended to apply, and you were informed the clause was included. Apparently, it was sent out to your customers, and you did not know it was in there, the clause, as customers often do not know these forced arbitration clauses are in there, the fine print. And I assume you are more sophisticated in these financial instruments and transactions than most of your customers, but leave that alone.

You were informed the clause—and clause was included because it was, quote, your words, "essentially 'cut and pasted' from a different Equifax offering." But this inadvertent error could have prevented, if not—if not unearthed and then protested, then pushed back and you dropped it, this inadvertent error could have prevented 145 million victims from pursuing their legal rights in court.

So make that case again. Your company failed by allowing this breach of 145 million victims. You sent out a piece. You sent out a restitution to them with forced arbitration. You backed off the forced arbitration.

So do not you think it is fundamentally unfair that the ability of 145 million Americans to seek justice in court could have been taken away simply by a cut-and-paste job? Does not that show how unfair forced arbitration is to customers?

Mr. SMITH. Senator, to be specific to this particular issue, it was an error, as you noted. We were made aware of the error, and I believe within 24 hours removed that clause. It was never intended to be a clause applied to the breach.

Senator BROWN. But that was not really the question.

So, first of all, you say it was an error. I guess I believe that, that it was an error, although your company has given us cause to not believe some other things. But does not that show how unfair forced arbitration is? You did not ask—you did not answer that question. If this inadvertent error, this cut-and-paste error had taken away forced—forced arbitration of 145 million Americans, does not that show how unfair forced arbitration is?

Mr. SMITH. I have no opinion on that.

Senator BROWN. But you used forced arbitration in other cases?

Mr. SMITH. Correct.

Senator BROWN. So you must not think it is—so it is unfair to those 145 million in that circumstance, but it is not unfair to customers in other circumstances on whom you oppose forced arbitration, both?

Mr. SMITH. Again, I go back, Senator. It was never the intent for us to have that arbitration clause in the breach service itself.

Senator BROWN. And I will close, Mr. Chairman. I appreciate your indulgence.

I just cannot understand why you think—for those 145 million in that case that forced arbitration is unfair, but in other uses in your company, you seem to think it is fair. It just puzzles me.

Senator BROWN. Senator Heitkamp.

Senator HEITKAMP. Thank you, Mr. Chairman.

And I just wanted to come back and offer a couple suggestions because we are all struggling, and obviously, your company has had a huge hit to its reputation.

We found out today that the IRS has been forced to continue your contract by your protest. That is why that contract was continued, and we, in spite of some very interesting timelines, the belief that you have that there was no insider training—and so I am just going to offer a couple of suggestions for you.

Number one, tell the IRS it is OK to migrate the contract someplace else and say, "We are fixing, getting our house in order. We understand that we have a ways to walk back, our reputation, and we are going to withdraw our protest on the loss of that contract."

And the other thing I would suggest to the three individuals, who may be completely innocent—but the rest of the shareholders who took the hit—they are more innocent than employees of that company, of your company—they should give the money back. They should give the money back.

And so I think there is other things. I think there is an attitude that we come here, we do everything possible, we are trying to do our level best, but many, many times, it is the symbolic things. It is like forcing the IRS to take this contract for another year, like a very suspicious timeline that has led us all to believe that there should at least, at a minimum, be an investigation. All of that could be undone with a gesture of goodwill.

And so I understand you are not the CEO of the company. You said you are still in an advisory role. My advice to you is do some

things that are very, very visible, and those are two things that you could do that would give us some certainty that this is being taken as seriously as it what it should be taken.

Thank you, Mr. Chairman.

Chairman CRAPO. Thank you.

And I will conclude with 3 minutes of questions as well.

Mr. Smith, I wanted to get back to my original question. A lot of the questions you have gotten today appropriately have been very specific with regard to Equifax and the Equifax breach.

I want to focus on the broader issue as we conclude. In my initial questioning to you, I talked to you about whether there were—whether any Experian data went to other entities, and I was referring to governmental entities—the CFPB, the Federal Reserve. We just had discussion about the IRS, and there are contractual relationships, I understand, with the use of this data.

Let me just talk about a the CFPB as an example. In September of 2014, the GAO did a report which I requested for on CFPB data collection. They found that CFPB at that time—that is 3 years ago now—had access to account-level credit card data on between 546 to 596 million consumer accounts on a monthly basis, representing 87 percent of the credit card market. GAO also found that at that time, there was not adequate protection at the CFPB of this data that they were collecting.

In this report, it indicated—again, this was in 2014—all of the sources of data that the CFPB was collecting—and Experian shows up in that report—700,000 vehicles per month, information procedure from Experian, vehicle purchases, and the data on those purchases, 10.7 million consumers, cosigners, and borrowers with consumer credit information from Experian, and another 600,000 samples of consumer credit reports and consumer credit scores on those reports from Experian.

Now, Experian is not the only entity that is providing data to the CFPB. There are, in this same report, for example, nine unidentified large financial institutions using a commercial data aggregator who provided 25 to 75 million total account sets of data involving individual consumers' credit card account-level data with linkages to their credit reporting data.

The reason, what I am getting into here, is this. Experian is not the only company or entity in America collecting data. There is massive data collection being undertaken in this country, and it is not just the three credit bureaus that are collecting this data.

I believe that Congress need to address not only the issue with Experian, but the broader issue of the collection and use and protection of personally identifiable information that is being collected by the Government, by the private sector, and others with regard to this personally identifiable data.

And I guess this is really more of a statement than a question, but I would like to know your opinion on that. Well, actually, there is a question first, and that is, Does Experian face requests from Federal regulators that are mandatory to provide data to them?

Mr. SMITH. Senator, Mr. Chairman, I assume you mean Equifax?

Chairman CRAPO. Yes. Excuse me.

Mr. SMITH. Yes.

Chairman CRAPO. Equifax.

Mr. SMITH. A general observation, a reaction to your thoughts there, if there was a better way to ensure that those that aggregate and manage significant amounts of data like we do, banks do, others in the industry, we would welcome that dialogue if there is a better path forward.

But to answer your question specifically, do we aggregate and provide data to different Government entities, the answer is yes.

Chairman CRAPO. All right. Thank you.

And I apologize. In fact, I gave the Experian examples, and that was just a mistake.

But your answer is that, yes, Equifax also provides data to those regulators, and it is not always voluntary, is it? In other words, you must provide it on occasion when it is required from agencies?

Mr. SMITH. Yes.

Chairman CRAPO. So let me ask you the general question, then. As Congress looks at this issue, it seems to me that it should be obvious that we should look much more broadly than even just one private-sector company and even then just the private sector, but to the data collection that is going on across our society, including the data collection that the Government itself is collecting. Would you agree?

Mr. SMITH. The rate and pace of cyberattacks is increasing at a rate that is unbelievable. If there is a way for public–private partnership to intelligently sit around a table and debate that and find better ways to manage and secure data, we would welcome that dialogue.

Chairman CRAPO. Thank you.

And I note that Senator Sasse came in, so he will get the last word. We are doing a 3-minute round, Senator Sasse.

Senator SASSE. Thank you, Mr. Chairman, and I would like to just associate myself with your comments right there about the digital revolution moment we are at, and the speed and pace of data aggregation and collection should push the Congress to have some real hard discussions about data ownership and transmission and implicit contracts where individuals are not contracting with one of the three credit bureaus and their data is still being managed and shipped in ways that they cannot control. I agree with you that we should have hearings and a lot of debate about this important topic in the digital revolution.

Mr. Smith, I want to just see if I can be clear about where I think we stand nearly 2 hours into this hearing. Your company, which has only two competitors, right? Really you only have two competitors—has lost the data of 145 million Americans, and this is not a spreadsheet problem. This is a real human problem where 2 and 3 and 4 years from now, you are going to have real Americans whose identity is going to be stolen, and their credit is going to be abused in the future. And they are going to have difficulty qualifying for a home loan or a car loan or they are going to pay a differential interest rate than they should be paying because of the rotten credit score that they are going to have.

And in response, your company could potentially make a profit from selling LifeLock products. Again, I agreed with you earlier that a lot of the forward-looking innovation that may come from this could incrementally improve things, but I think we are most

interested right now in the retrospective moment for these 145 million.

You are going to have a product that could potentially be sold to the very victims. It feels like a broken-windows business model where you did not actively chuck the bricks, but your company allowed bricks to be tossed through windows, and then you might potentially be able to sell new windows to some of the same people whose windows were just broken.

And I think the way you explained your LifeLock product in your testimony makes some sense for what you plan to roll out in January of 2018, but it is still really hard to understand it as a fraud protection product when you think about the victims historically. So I want to go back for just a minute to this contract with the IRS.

So we checked, and it appears to be a no-bid, even if it is a revolving contract that is a no-bid, but the purpose of the contract with the IRS looks like it is fraud prevention, right? You are trying to prevent fraudulent access.

I will not ask for a show of hands in the room, but I do not know who would want to say we should buy fraud protection from the people who were just hacked and dumped 145 million American records.

So just honestly as an American—and I appreciate the fact that you have resigned from the company, but as an American, why should anybody hire Equifax for fraud protection right now after the exposure?

Mr. SMITH. Senator, I understand your point. We are a company that has been around for 118 years and for most of those 118 years have done good things for many stakeholders, including the Government, and one of those things we have done very proudly is prevent fraud for many entities, including the Government.

I come back. It was a horrific breach, and I apologize on behalf of the company for that breach. We will make it right as best we can, but it does not wipe out 118 years of good work we have done.

Senator SASSE. Thank you.

I am going to be following up with the IRS and asking them why this contract should go forward, but thank you for your willingness to appear before the Committee today.

Mr. SMITH. Thank you.

Chairman CRAPO. Thank you, Senator.

And that concludes the questioning.

Mr. Smith, we do appreciate you coming before the Committee and appearing today.

For all Senators, all follow-up questions need to be submitted by next Wednesday, October 11th.

And, Mr. Smith, we ask that you please respond promptly to those questions. We usually like to see the responses within a week, if possible.

With that, this hearing is adjourned.

Mr. SMITH. Thank you.

[Whereupon, at 12:01 p.m., the hearing was adjourned.]

[Prepared statements, responses to written questions, and additional material supplied for the record follow:]

PREPARED STATEMENT OF RICHARD F. SMITH

FORMER CHAIRMAN AND CHIEF EXECUTIVE OFFICER, EQUIFAX, INC.

OCTOBER 4, 2017

Preliminary Statement

Chairman Crapo, Ranking Member Brown, and Honorable Members of the Committee, thank you for the opportunity to testify today.

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, though 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*, 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 con-

sumers 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 2 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 2 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 back-end 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 back-end 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 Crapo, Ranking Member Brown, 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 8 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 2 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.

RESPONSES TO WRITTEN QUESTIONS OF THE SENATE BANKING COMMITTEE FROM RICHARD F. SMITH

KING & SPALDING

King & Spalding LLP
1700 Pennsylvania Ave, NW
Washington, D.C. 20006-4707
Tel: (202) 737-0500
Fax: (202) 626-3737
www.kslaw.com

Theodore M. Hester
Direct Dial: 202-626-2901
thester@kslaw.com

VIA E-MAIL

December 22, 2017

Confidential Treatment Requested
All Rights Reserved

The Honorable Mike Crapo, Chairman
Committee on Banking, Housing,
and Urban Affairs
United States Senate
534 Dirksen Senate Office Building
Washington, D.C. 20510

RE: Equifax's Submission in Response to Committee Requests Dated Oct. 12, 2017

Dear Chairman Crapo:

On behalf of our client, Equifax Inc. ("Equifax" or the "Company"), I am writing in response to your October 12, 2017 letter requesting responses to questions from the Committee following the Committee's October 4, 2017 hearing entitled, "*An Examination of the Equifax Cybersecurity Breach.*" Pursuant to ongoing communications with Committee staff, Equifax has asked me to formally submit information responsive to your questions for the record (see attached Appendix A). Today's submission supplements information Equifax has provided to the Committee at the hearing on October 4, through briefings provided to the Committee staff on September 11 and September 21, and in our October 1 written response. Equifax will provide additional responses when it is able to do so.

In responding to the Committee's questions at the October 4 hearing, Mr. Smith used his best efforts to be as accurate and responsive as possible based on his knowledge and recollection of the facts. Similarly, in responding to the Committee's subsequent requests, Equifax has used its best efforts to be as accurate and responsive as possible based on its understanding of the terms used in your letter. The representations herein are based on reasonably available information and are not intended to, and do not, capture every event related to Equifax's ongoing investigation, nor are they an exhaustive description of the events discussed. In providing these responses, Equifax does not waive, nor does it intend to waive, any of its rights or privileges with respect to this inquiry, including any applicable attorney-client, work product or other evidentiary privilege, or any objections to the assertions or requests in your letter. We respectfully request advance notice of any contemplated disclosure of the Company's

confidential, trade secret, and proprietary information, and a reasonable opportunity to object. Please direct any such notice to me at the above address.

Should you have any questions concerning the information provided herein, please contact me directly at 202-626-2901.

Sincerely,

Theodore M. Hester

cc: Senator Sherrod Brown, Ranking Member
Senator Jack Reed
Senator Robert Menendez
Senator Jon Tester
Senator Mark Warner
Senator Elizabeth Warren
Senator Heidi Heitkamp
Senator Joe Donnelly
Senator Brian Schatz
Senator Chris Van Hollen
Senator Catherine Cortez Masto
Senator Ben Sasse
Senator Richard Shelby

Enclosure

Appendix A

EQUIFAX'S SUBMISSION IN RESPONSE TO COMMITTEE REQUESTS DATED OCTOBER 12, 2017

Please note that the question numbers are not the Committee's question numbers, but are being provided for ease of reference.

Equifax is providing the Committee with a copy of the Special Committee Report referenced throughout the responses provided below (attached to this letter) and is producing documents Bates numbered EFXCONG-SBC000000001 to EFXCONG-SBC000000185 to the Committee as part of today's production. Due to email file size limitations, Equifax is producing the Bates numbered documents to the Committee on a CD, which has been encrypted to ensure the privacy and integrity of the data. The password to gain access to the materials will be sent by separate correspondence.

Questions for Mr. Richard F. Smith, Former Chairman and Chief Executive Officer of Equifax, Inc. on behalf of Ranking Member Brown, Senator Jack Reed, Senator Robert Menendez, Senator Jon Tester, Senator Mark Warner, Senator Elizabeth Warren, Senator Heidi Heitkamp, Senator Joe Donnelly, Senator Brian Schatz, Senator Chris Van Hollen, and Senator Catherine Cortez Masto:

Question #2 (p. 2): We know the decision was not yours, but given the singular importance of protecting private data to Equifax's business model, do you think it is appropriate that you were awarded this compensation?

A: As a threshold matter, Mr. Smith does not believe the various reports regarding his compensation between 2016 and 2017 are accurate. In addition, his compensation structure was determined by an independent committee of the Board of Directors, elected by the Company shareholders, and was aligned with the performance of the Company.

Question #5 (p. 3): Given your testimony that Equifax's consumer-facing segment comprises a small portion of the company's overall business, how does your compensation package's focus on shareholder return ensure that the company takes adequate precautions against theft of consumers' personal identifying information?

A: Equifax is a 118-year-old company, that prides itself on being a trusted steward of data, regardless of whether it is a consumer's data or a company's data. The Company's business model depends on it and the reputational impact of a data breach is just as significant coming from a consumer breach, as it is with a corporation breach. Aligning the executive's compensation with building long term value for shareholders is good corporate governance and is consistent with this model. The Company's compensation structure reflects that.

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC.

Question #6 (p. 3): Your compensation package appears to have incentivized the pursuit of short-term revenue growth, profits, and stock returns over protection of consumer information. What changes in law would ensure that consumer reporting agencies' primary focus is protecting consumers and ensuring credit-report accuracy?

A: With respect to Mr. Smith's compensation, Equifax respectfully submits that a large majority of his compensation (over 70%) was based on three-year share performance, rather than short-term revenue growth or profits. This three year performance metric directly aligns his compensation with the value delivered to shareholders. Only a small portion of Mr. Smith's compensation was based on short-term performance.

In establishing and reviewing Equifax's executive compensation program, the Compensation Committee of the Board of Directors considered whether the program encourages unnecessary or excessive risk-taking and concluded that it does not. The Compensation Committee also considered shareholder feedback in its review of the compensation program, as well as compensation plan and benchmarking advice from its independent compensation consultant. Further, the shareholders of Equifax confirmed their support for the Company's executive officer compensation plan by overwhelmingly approving the compensation package at the last annual meeting of shareholders held on May 4, 2017.

Equifax understands that being the holder of consumer information and data carries with it enormous responsibility. Equifax has devoted substantial resources to this area historically and, as described in more detail throughout the other responses, Equifax has taken a number of important steps to enhance consumer data protection and will continue to implement additional improvements going forward.

Equifax and consumers have an aligned interest in ensuring credit report accuracy; it is in Equifax's business interest to maintain a high level of accuracy in the reports that it provides to lenders and other authorized customers. Based on the foregoing, Equifax believes that a change in law is not necessary to ensure its focus on these important matters.

Question #8 (p. 4): In an August Q&A at the University of Georgia, you stated that traditionally, Equifax has "owned [consumers'] credit data." You also mentioned the potential for a new regulatory model in which consumers own this data: "[T]here's going to be a time—and it's going to be sooner rather than later, because it's occurring in the U.K. right now—where through regulation, the U.K. regulators are saying, 'No, no. You no longer have the rights to own that data.'" This appears to be a reference to the United Kingdom's planned 2018 implementation of the E.U. General Data Protection Regulation (GDPR). The GDPR grants consumers several rights that do not exist under current U.S. law, including the right to make companies delete their personal data. Rather than characterizing this new legal regime as an insurmountable obstacle for Equifax, you championed the technological responses Equifax could take and framed the regulatory change as a potential "opportunity." This is consistent with the tone of a short article by

Trevor Parker, Chief Compliance Officer at Equifax (entitled "The Future of Data Protection"), which states that companies must be "ready" for GDPR compliance. How will Equifax's U.K. businesses adapt to be "ready" for the GDPR?

A: Equifax's current analysis indicates that its U.S. operations do not process data that is subject to the extraterritorial application of GDPR. As such, Equifax is taking measures to comply with its contractual obligations under data processing agreements with data controllers or processors that have indicated that the data they provide to Equifax for processing in the U.S. is subject to GDPR.

In the U.K., Equifax has been investing and working on its GDPR compliance project since 2016, including following the 12-step approach as outlined and promoted by the U.K. data protection regulator, the Information Commissioner's Office ("ICO").

These actions include reviewing and updating (as appropriate) contractual arrangements with clients, suppliers, and processors with up-to-date GDPR contractual terms and ensuring contractual terms include cooperation and assistance provisions between the parties so that Data Subject Rights (including the right of erasure) can be fulfilled where appropriate and required.

In addition, regarding the right of erasure, Equifax is working on a joint exercise with the other U.K. CRAs, the ICO and key financial services clients to implement a standard U.K. Credit Reference Agency Information Notice ("CRAIN") that all credit data sharers will utilize in their interactions with their customers post-GDPR. This standard will help ensure the ongoing, lawful sharing and processing of credit report information.

In Iberia, Equifax has also been working on its GDPR compliance project since 2016. In common with the U.K., this activity includes reviewing and updating (as appropriate) contractual arrangements with clients, suppliers, and processors with up-to-date GDPR contractual terms. In addition to the requirements of the GDPR, a forthcoming Spanish data protection regulation will affect the business.

The review of operations includes the right of erasure in respect of both "negative" (missed payments) and "positive" bureau data, to which different procedures apply.

Equifax is taking the necessary steps toward achieving compliance with GDPR on or before the May 2018 deadline.

Question #9 (p. 4): Do you believe that if the United States adopted a legal framework in which consumers own their data and can make companies erase it, Equifax could adapt to those changes? You may explain your answer, but please state an ultimate "yes" or "no" conclusion. If the answer is no, please explain why Equifax's U.K. business will survive the U.K. implementation of the GDPR but Equifax's U.S. business could not withstand a similar change in U.S. law.

A: Harmonizing data protection standards could eliminate some of the friction in doing business across borders, and lead to synergies that could ultimately benefit consumers. Equifax is committed to the best interests of consumers, including data protection, in every aspect of its global operations. Equifax would gladly participate in discussions with the goal of bringing data protection standards in the U.S. and the EU closer together.

In your testimony, you claimed that Equifax is a "vital part" of "the global economy" and "provide[s] a great service to the consumer, enabling them to get access to credit." In your August Q&A at the University of Georgia, you stated that Equifax does not enter some markets because of an unfavorable regulatory environment.

Question #10 (p. 4): Are there countries with well-developed consumer credit markets where Equifax maintains no presence?

A: Equifax operates or has investments in 24 countries in North America, Central and South America, Europe, and the Asia Pacific region. These countries represent both developed and emerging markets with credit economies at various levels of maturity. There are several countries in which Equifax does not operate that have established credit markets, many of which are in Europe and Asia.

Question #12 (p. 4): It is a stated priority of the Consumer Data Industry Association, of which Equifax is a member, to get consumers out of payday loans and into the regulated banking industry. Does Equifax support the CFPB's payday-loans rule?

A: Equifax does not oppose or support the CFPB's payday-loans rule. Equifax submitted constructive comments to assist the Bureau in its regulatory promulgation. These comments focused on the proposed Registered Information System and the ability-to-repay provisions. Per the CFPB's request, Equifax also participated in ex parte communications with the Bureau to provide insight and feedback on the proposed rule's requirements.

Senator Cassidy and Senator Brown wrote to the Social Security Administration (SSA) to ask whether Social Security numbers in the SSA's E-ID Verify program, which is run by Equifax, were compromised. According to the SSA, Equifax stated that it "found no evidence that this incident impacted any information provided to Equifax by the [SSA]." The day before the hearing, Politico reported that Equifax was being granted a multimillion-dollar fraud-prevention contract with the IRS. This means that two federal agencies responsible for safeguarding Americans' most sensitive information are relying on Equifax to protect this information. It took Equifax months to discover and assess the breach that exposed 145.5 million Americans' Social Security numbers and other personal information to identity thieves. Additionally, security expert Brian Krebs reports that "Equifax's poor security contributed to an epidemic of tax refund fraud at the IRS in the 2015 and 2016 tax years, when fraudsters took advantage of weak security questions provided to the IRS by Equifax to file and claim phony tax refund requests on behalf of hundreds of thousands of taxpayers."

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC.

Question #13 (p. 4): How can we trust that contracting with Equifax does not put the IRS and SSA—and Americans' most sensitive personal information—at risk for future breaches? Will Equifax be implementing additional security procedures?

A: Equifax remains confident in its ability to provide services to the IRS and SSA. Equifax has taken important steps to improve its data security infrastructure. It is further hardening its networks, changing its procedures to require "closed loop" confirmation when software patches are applied, rolling out new vulnerability detection tools, and strengthening accountability mechanisms. Equifax has implemented certain technological remediation steps as described in the Mandiant executive summary, which was submitted to this Committee on October 1, 2017. Equifax has 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.

Question #14 (p. 4): Please list all Equifax consumer products for which the contract, terms of service, or any other agreement contains a forced-arbitration clause.

A: Equifax has over 50 direct-to-consumer products that provide consumers with a wide variety of credit monitoring features, identity theft protections, and other credit report services through both subscription-based and transactional, one-time offerings. This includes products sold under the Equifax, TrustedID (including co-branded partner products), and ID Watchdog brands.

All Equifax direct-to-consumer products described above currently contain an arbitration provision in the product Terms of Use, except for the following specific products:

- **TrustedID Premier** – a complimentary identity theft protection and credit file monitoring product offered to all U.S. consumers
- **TrustedID Essentials** – a TrustedID credit monitoring product
- **Equifax CreditWatchTM Gold with 3-in-1 Monitoring** – a complimentary identity theft protection and credit file monitoring product offered via direct mail for consumers without online access
- **Comerica IDMonitor** – a TrustedID-supported partner credit monitoring product
- **AARP® Identity Theft Protection** – a TrustedID-supported partner credit monitoring product

Enrolling in TrustedID Premier, which is being offered to U.S. consumers since the cybersecurity incident, does not prohibit consumers from taking legal action. Moreover,

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC.

the Terms of Use on www.equifax.com do not apply to the TrustedID Premier product being offered to consumers as a result of the cybersecurity incident, and the arbitration provision included in those terms does not apply to claims related to the cybersecurity incident.

Question #15 (p. 5): Please list all Equifax consumer products for which the contract, terms of service, or any other agreement contains a forced-arbitration clause.

A: Please see response to Question #14.

Question #16 (p. 5): Do Equifax's employment agreements or other arrangements with nonexecutive employees contain forced-arbitration clauses?

A: No.

Question #17 (p. 5): Will Equifax voluntarily remove forced-arbitration clauses from all of its consumer products?

A: Equifax is not currently offering any subscription services to consumers for purchase. Equifax will not include an arbitration clause in connection with the forthcoming credit lock application that will be available in January 2018.

Question #18 (p. 5): Is there any data that is so deeply personal or of such an intimate nature that Equifax will not collect it, even if collecting the data were legal?

A: Equifax does not have any standing principals that would prohibit it from collecting specific types of data where it is legal to do so. For each potential data element, Equifax considers a number of factors about the data, including existing regulations, the ability to govern the quality and consistency, the availability of sufficient depth and coverage, and consumer benefit. Where the confluence of these factors leads Equifax to reject a data element, Equifax manages its response centrally to ensure consistency among each business unit.

Question #19 (p. 5): Federal filings show that before the breach, Equifax lobbied on a House bill that would thwart consumers' ability to hold consumer reporting agencies accountable for FCRA violations. Please describe any lobbying activity by Equifax, its affiliates, or its agents between July 1, 2017 and October 11, 2017 (including the approval of lobbying expenditures and any meetings between lobbyists and lawmakers). In each case, please state (1) the date of the expenditure approval or meeting, as the case may be; (2) the bill, rule, or matter at issue; (3) the houses of Congress and federal agencies lobbied; (4) the individual(s) who made the decision to lobby; (5) when the individual(s) who made the decision to lobby became aware (a) of the "suspicious activity" to which you referred in your testimony and (b) that this suspicious activity may have exposed consumers' personal information; and (6) whether and when you and the current interim CEO became aware of the lobbying decision or meeting, as the case may be.

A: The chart below includes the meetings that Equifax participated with congressional offices related to Fair Credit Reporting Act ("FCRA") reform, or H.R.2359, for the time period of July 1, 2017 through October 11, 2017. During this period, Equifax participated in other lobbying activities such as preparing background documents, exchanging emails, and participating in conference calls. Following the announcement of the cybersecurity incident on September 7, 2017, all communications related to H.R.2359 were limited to responding to inquiries.

Meeting Date	Chamber
July 6, 2017	House
July 10, 2017	Senate
July 11, 2017	Senate & House
July 14, 2017	Senate
August 3, 2017	House
August 22, 2017	House
August 23, 2017	House
August 30, 2017	House
August 31, 2017	House
September 1, 2017	House
September 5, 2017	House
September 6, 2017	House

The Senior Vice President for External Affairs makes the decision to lobby on an issue and provides updates to the Legal Department on a regular basis. The Chief Executive Officer was not made aware of individual meetings, lobbying activities or legislative objectives. The Senior Vice President for External Affairs was made aware of suspicious activity on August 23, 2017. Because of the sensitive nature of the incident, the Senior Vice President for External Affairs was prohibited from communicating this material, non-public information to others and has not participated in lobbying activity since August 23, 2017.

Equifax provided notice of the cybersecurity incident to the lobbyists it employed on September 6, 2017. Notice of the cybersecurity incident was provided to external consultants and lobbyists on September 7, 2017. Expenditures for these meetings were limited to travel costs and salary for lobbyists employed by Equifax. External consultants and lobbyists are generally on monthly retainer arrangements and only reimbursed incidental, negligible costs for individual meetings.

Question #20 (p. 5): Federal filings show that before the breach, Equifax and the Consumer Data Industry Association lobbied on a Consumer Financial Protection Bureau rule that would prohibit forced arbitration in consumer contracts, including credit monitoring products like those Equifax offered after the breach. Please describe any lobbying activity by Equifax, its affiliates, or its agents between July 1, 2017 and October

11, 2017 (including the approval of lobbying expenditures and any meetings between lobbyists and lawmakers). In each case, please state (1) the date of the expenditure approval or meeting, as the case may be; (2) the bill, rule, or matter at issue; (3) the houses of Congress and federal agencies lobbied; (4) the individual(s) who made the decision to lobby; (5) when the individual(s) who made the decision to lobby became aware (a) of the "suspicious activity" to which you referred in your testimony and (b) that this suspicious activity may have exposed consumers' personal information; and (6) whether and when you and the current interim CEO became aware of the lobbying decision or meeting, as the case may be.

A: Lobbyists employed by Equifax attended two industry-wide meetings on July 11, 2017 with the Senate regarding several topics impacting the credit reporting industry, including the use of arbitration agreements and House Joint Resolution 111. Equifax also participated in industry-wide calls in which the topic of arbitration clauses was addressed.

The Senior Vice President for External Affairs makes the decision to lobby on an issue and provides updates to the Legal Department on a regular basis. The Chief Executive Officer was not made aware of individual meetings, lobbying activities or legislative objectives. The Senior Vice President for External Affairs was made aware of suspicious activity on August 23, 2017. Because of the sensitive nature of the incident, the Senior Vice President for External Affairs was prohibited from communicating this material, non-public information to others and has not participated in lobbying activity since August 23, 2017.

Equifax provided notice of the cybersecurity incident to the lobbyists it employed on September 6, 2017. Notice of the cybersecurity incident was provided to external consultants and lobbyists on September 7, 2017. Expenditures for these meetings were limited to travel costs and salary for lobbyists employed by Equifax. External consultants and lobbyists are generally on monthly retainer arrangements and only reimbursed incidental, negligible costs for individual meetings.

Question #21 (p. 6): Will Equifax commit to paying for consumers' credit locks or freezes at Experian and TransUnion?

A: Equifax is committed to working with the entire industry, including Experian and TransUnion, to develop solutions to cybersecurity and data protection challenges we all face. Equifax is offering consumers TrustedID Premier, a free package of services that it believes will substantially mitigate the risk of harm to consumers. Beginning at the end of January, consumers will have the ability to lock and unlock their Equifax credit report for free, for life.

Question #27 (p. 7): On what dates did specific personnel and divisions become aware of the incident?

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.

CEO Richard Smith was told about the suspicious activity the next day, July 31, in a conversation with the Chief Information Officer. At that time, Mr. Smith was informed that there was evidence of suspicious activity on the dispute portal and that the portal had been taken offline to address the potential issues.

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) engaged, through company counsel, the independent cybersecurity forensic firm, Mandiant, to investigate the suspicious activity; and (3) contacted the Federal Bureau of Investigation ("FBI").

Over the next several weeks, Mandiant and Equifax's security department analyzed forensic data seeking to identify and understand these early indications of unauthorized activity on the network. Their task was to figure out what happened, what parts of the Equifax network were affected, identify consumers that were impacted, and what 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 ("PII"), 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 17, Equifax senior leadership team met to receive a 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. The company had expert forensic and legal advice, and was mindful of the FBI's need to conduct its criminal investigation.

On August 22, Equifax's presiding director of the Board of Directors, Mark Feidler, was notified of the data breach, as well as Mr. Smith's direct reports who headed up various business units. In special telephonic board meetings on August 24 and 25, the full Board of Directors was informed. Equifax also began developing the remediation needed to assist affected consumers, even as the investigation continued.

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC.

By September 4, the investigative team had created a list of approximately 143 million consumers whose personal identifying information was believed to have been impacted, and Equifax continued its 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, 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.

On September 7, 2017, Equifax provided notification of the incident by issuing a nationwide press release, providing the dedicated website where consumers could determine if their personal identifying information was impacted and sign up for the credit file monitoring and identity theft protection product, and providing a dedicated call center for consumers. The notification indicated that the incident impacted personal identifying 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. On October 2, 2017, following the completion of the forensic portion of the investigation of the incident, Equifax announced that approximately 2.5 million additional U.S. consumers were potentially impacted, for a total of 145.5 million.

Question #28 (p. 7): On what dates were specific personnel informed that more than 100,000; more than 1,000,000; more than 25,000,000; more than 50,000,000 and more than 100,000,000 consumers were affected?

A: Please see response to question #27, which provides information about how Equifax became aware of the number of consumers affected.

Question #29 (p. 7): How was the incident response process coordinated internally between relevant divisions?

A: Please see response to question #27.

Question #31 (p. 7): When you and senior management first learned of the breach, to whom and how was that information communicated, and were subsequent actions taken by you and other senior management?

A: Please see response to question #27.

Question #33 (p. 7): Please provide a description of the cybersecurity oversight and policies and procedures that Equifax had in place prior to the detection of the breach and updates or other changes the company has instituted since.

A: Equifax has a formalized security program supported by administrative, technical, and physical safeguards focused on the protection of consumer data. Equifax has a

security team in place, which is responsible for the coordination and execution of the Company's information security program. The security team reports to Equifax's Chief Security Officer and operates using defined plans and procedures for responding to security incidents, which are revised on a regular basis. Security incidents are classified according to severity and escalated to management personnel as appropriate. The security team includes dedicated incident response managers and a Cyber Threat Center, which is staffed by security professionals and uses technological capabilities to monitor the Company's network. Equifax has physical safeguards in place to secure its data centers.

Equifax has taken important steps to improve its data security infrastructure. It is further hardening its networks, changing its procedures to require "closed loop" confirmation when software patches are applied, rolling out new vulnerability detection tools, and strengthening accountability mechanisms. Equifax has implemented certain technological remediation steps as described in the Mandiant executive summary, which was submitted to this Committee on October 1, 2017. Equifax has 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.

Question #34 (p. 7): Please explain specifically how Equifax systems were breached, including how intruders were able to enter Equifax's system, what vulnerabilities were exploited, how intruders were able to access data, and a list of all data sources, databases, or tables containing personally identifiable information that were accessed.

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. For your reference, Equifax provided copies of the executive summary and supplemental report to the Committee on October 1, 2017 and a copy of the final supplement to the Committee on October 6, 2017.

Equifax's internal investigation of this incident is ongoing and the Company continues to work closely with the FBI in its investigation.

Question #35 (p. 7): Please provide a complete list of all types of personally identifiable information that was compromised. Please describe your long term plans to address risks and harm to consumer including any resources set aside for future compensation and remediation for victims.

A: On September 7, 2017, Equifax publicly announced that the breach impacted personal information primarily including names, Social Security numbers, birth dates, addresses and, in some instances, driver's license numbers. Credit card numbers and information contained on dispute documents were also impacted for some consumers. 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

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC.

final supplement. For your reference, Equifax provided copies of the executive summary and supplemental report to the Committee on October 1, 2017 and a copy of the final supplement to the Committee on October 6, 2017.

Equifax has implemented certain technological remediation steps as described in the Mandiant executive summary and the Company is working with federal and state regulators, as well as consumer stakeholders, regarding remediation steps.

Questions for Mr. Richard F. Smith, Former Chairman and Chief Executive Officer of Equifax, Inc. from Senator Cortez Masto:

Question #36 (p. 8): When can I expect a substantive response to my letter dated September 11th, 2017 regarding Equifax's position on mandatory pre-dispute arbitration clauses and S.J. 47, Senate legislation seeking to nullify the Consumer Financial Protection Bureau's rule limiting use of such clauses?

A: Equifax is not currently offering any subscription services to consumers for purchase. Equifax will not include an arbitration clause in connection with the forthcoming credit lock application that will be available in January 2018.

Question #37 (p. 8): Equifax executives sold stock in the company on August 1st and August 2nd. Per your testimony to the Senate, this stock sale was approved by Equifax's Chief Legal Counsel. Equifax also contacted the Federal Bureau of Investigations (FBI) and Mandiant on August 2nd. Was the Chief Legal Counsel who approved of the stock sales also aware that the firm contemporaneously contacted the FBI and Mandiant? Did the Chief Legal Counsel approve any contracts with Mandiant related to the July 29th "suspicious traffic?"

A: The Equifax Legal Department approvals of the referenced stock sales were not made "contemporaneously" with the contacts with the FBI and Mandiant, as further explained below.

The Board of Directors of Equifax released a report by a Special Committee of the Board of Directors 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 that two of the executives whose trades were reviewed received clearance from Legal Department personnel on July 31, 2017, and two other executives received Legal Department clearance on August 1, 2017.

Based on the early indications of suspicious activity, on August 2, 2017, (1) the Company's Senior Vice President, U.S. Legal—on behalf of Equifax—retained the cybersecurity group at the law firm of King & Spalding to guide the forensic investigation and provide legal and regulatory advice; (2) King & Spalding engaged the independent cybersecurity forensic firm, Mandiant, to aid in investigation of the suspicious activity; and (3) the Company contacted the FBI. It was not until later in August that the forensic investigation determined the hackers may have accessed a database table containing a large amount of consumers' PII, and potentially other data tables. The Chief Legal Officer was not aware of these engagements or the contact of the FBI before they were made, but became aware of them after they occurred.

The Chief Legal Officer was not involved in reviewing or approving the agreement with Mandiant. The Company's Vice President Legal reviewed and approved the agreement.

Question #38 (p. 8): What resources is Equifax making available to ensure that community banks and credit unions are made whole as a result of this data breach?

A: Following the announcement of the cybersecurity incident, Equifax has met with and continues to work with community banks and credit unions to provide them information about the cybersecurity incident and to respond to specific questions raised. Equifax also made available communication materials (i.e., FAQs) to the community banks and credit unions that provide information about the cybersecurity incident to their customers and members. Equifax continues to accommodate requests from community banks and credit unions to further discuss the cybersecurity incident.

Question #40 (p. 8): What dividends did Equifax pay out to shareholders following knowledge of the data breach? Why did Equifax elect to pay out dividends to shareholders given knowledge of the company's tremendous legal exposure and the harm caused to consumers?

A: Since the Company's security team discovered the unauthorized access on July 29, it declared (1) a quarterly dividend on August 4, 2017 of $0.39 per share, which was paid on September 15, 2017, and (2) a quarterly dividend on November 9, 2017 of $0.39 per share, which is payable on December 15, 2017. Decisions regarding the declaration and payment of dividends depend on the Company's financial condition, earnings, prospects, current and future funding requirements, applicable law, and other relevant factors. The dividends paid in 2017 reflect consideration of these factors.

Question #41 (p. 8): Can Equifax provide data on the number of active duty servicemembers and seniors impacted by the data breach, broken down by state?

A: Active duty status is not a data element that Equifax possesses. As a result, Equifax is unable to calculate the number of active duty servicemembers impacted by the breach.

It is difficult to accurately assess the number of impacted seniors. The dates of birth included within the data associated with the cybersecurity incident consist of self-reported birth dates or not dates at all and as a result, the information may not be reliable for purposes of calculating the total number of seniors impacted by the incident. For example, some dates in the data do not appear to reflect accurate dates of birth (e.g., 1/1/1111).

Questions for Mr. Richard F. Smith, Former Chairman and Chief Executive Officer of Equifax, Inc. from Senator Robert Menendez:

Question #46 (p. 10): Equifax shareholders filed a resolution this year asking the company to disclose its political spending. Shareholders were prompted by the fact that Equifax devotes significant corporate resources on politics without disclosing it to shareholders.[1] In addition, Equifax does not disclose the money it gives to trade associations such as the Consumer Data Industry Association, which represents Equifax, Experian, and TransUnion, and has lobbied against the Consumer Financial Protection Bureau's forced arbitration rule. In light of the significant drop to Equifax stock prices following the data breach, do you believe that shareholders deserve to know when Equifax is actively fighting consumer protections and accountability at the expense of shareholders?

A: As described below and in Equifax's 2017 Proxy Statement, Equifax has disclosed appropriate information regarding its political contributions and has an appropriate system of oversight in place, including a formal Political Contributions Policy and Code of Ethics, to ensure that its political contributions comply with applicable law and are in the best, long-term interests of the Company and its shareholders.

- **Equifax has historically made an extremely limited number of political contributions of *de minimis* value**. Equifax's political contributions are not financially material to the Company. In 2016, 2015 and 2014, aggregate political contributions made directly by Equifax with corporate funds totaled approximately $1,500, $2,000, and $10,250, respectively. In 2016, Equifax's total expenses relating to political contributions were *de minimis* when compared to its total operating costs of approximately $2.3 billion.

- **Equifax is transparent and accountable regarding its political contributions.** Equifax operates in a highly-regulated industry, and the decisions of federal, state and local governments can significantly impact the Company. On a limited basis, Equifax has pursued and will continue to pursue efforts to help inform public policy decisions that have the potential to affect its industry, business, products, customers, employees, shareholders, and communities.

Equifax pays annual membership dues to industry trade associations. The trade associations in which Equifax participates may engage in political activities, but such decisions are governed by those associations' respective bylaws. Thus, even when Equifax participates in trade associations, it does not control how they use membership dues. Equifax expects that these trade associations comply with applicable laws with respect to their political activities. Equifax believes that additional disclosure regarding the specific payments made to these trade associations would not benefit shareholders.

- **Significant disclosure regarding the Company's political activities and related policies is already publicly available.** Please consider the following:

- Under federal law, all contributions by the Equifax Inc. Political Action Committee, the sole political action committee affiliated with the Company, are required to be reported, and a list of such contributions is publicly available at the website of the United States Federal Election Commission.

- As noted above, Equifax publicly discloses aggregate political contributions made directly by the Company with corporate funds for the most recently completed fiscal year. Contributions made directly by Equifax are typically small in amount and most frequently made to local- and state-level candidates.

- Federal law prohibits corporations from contributing corporate treasury funds to federal candidates or federal campaign committees. Accordingly, Equifax makes none.

- The Policy and the Code of Ethics are available on the "Corporate Governance" section of Equifax's website. The Governance Committee's oversight of the Policy, the Guidelines and Equifax's political engagement activities is memorialized in the Committee's written charter, which is also available on the Company's website.

Finally, the shareholder proposal described in the question above was presented at the last annual meeting of shareholders, held on May 4, 2017, and Equifax's shareholders chose not to approve the proposal.

Question #47 (p. 10): Please describe the policies in place during your tenure as chief executive officer pertaining to the permissibility of stock sales by senior management and leadership in near proximity to a significant announcement by the company.

A: Equifax has in place an insider trading policy that sets forth procedures governing employees' trading in the Company's securities, including:

(a) prohibiting all employees from trading while in possession of material, nonpublic information;

(b) permitting certain individuals (including, among others, officers and directors) to trade only during specified trading windows that follow the public release of quarterly financial information; and

(c) with respect to certain designated individuals (including Section 16 reporting officers, as well as directors), permitting trades only after obtaining pre-approval from the office of the Company's chief legal officer or his or her designee.

Equifax is producing a copy of this policy with this submission. The policy is Bates numbered EFXCONG-SBC000000001 to EFXCONG-SBC000000014.

Question #55 (p. 10): Please describe how active duty servicemembers were impacted by the data breach.

A: Active duty status is not a data element that Equifax possesses. As a result, Equifax is unable to calculate the number of active duty servicemembers that were impacted by the cybersecurity incident. However, based on the number of consumers that were impacted, it is highly likely that some were active duty servicemembers. Equifax's description of the incident and its impact on consumers would also apply to any active duty servicemembers that were impacted.

Question #56 (p. 11): How many active duty servicemembers were impacted by the data breach?

A: Active duty status is not a data element that Equifax possesses. As a result, Equifax is unable to calculate the number of impacted active duty servicemembers.

Question #57 (p. 11): What specific actions is Equifax currently taking to identify active duty servicemembers and provide appropriate remediation?

A: Equifax is strongly committed to helping military service members. The company has been in direct communication with the Department of Defense and CFPB's Office of Servicemember Affairs, and is working on efforts to further educate servicemembers, including those impacted by the cybersecurity incident, regarding the incident and the various options available to them, such as the free TrustedID Premier service, security freezes, and active duty alerts, as well as other relevant information.

In addition, in response to the cybersecurity incident, Equifax 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, including Veterans and servicemembers.

Question #58 (p. 11): In your opinion, to protect themselves from identity theft and fraud, how long do consumers impacted by the breach need a credit monitoring service? If longer than a year, will Equifax commit to providing such services at no cost to consumers impacted by the data breach?

A: Equifax is offering consumers TrustedID Premier, a free package of services that it believes will substantially mitigate the risk of harm to consumers. Beginning at the end

of January, consumers will have the ability to lock and unlock their Equifax credit report for free, for life.

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC.

Questions for Mr. Richard F. Smith, Former Chairman and Chief Executive Officer of Equifax, Inc. from Senator Jack Reed:

Question #60 (p. 12): Four days after announcing the cybersecurity breach, Equifax reversed itself by removing forced arbitration language from websites and products associated with the breach. If you concede that forced arbitration is bad for consumers you may have wronged, why doesn't Equifax stop using forced arbitration clauses in consumer contracts altogether?

A: Equifax is not currently offering any subscription services to consumers for purchase. Equifax will not include an arbitration clause in connection with the forthcoming credit lock application that will be available in January 2018.

Question #61 (p. 12): Do you personally believe that senior executives or shareholders should bear the costs associated with potential fines and penalties levied against Equifax for the cybersecurity breach, and why do you hold this view?

A: Mr. Smith has not had the opportunity to review your proposed legislation, but he believes it would be inappropriate to comment on the legislation or cost-sharing proposals in light of ongoing civil litigation relating to the 2017 breach.

Questions for Mr. Richard F. Smith, Former Chairman and Chief Executive Officer of Equifax, Inc. from Senator Ben Sasse:

Question #70 (p. 13): Has Equifax updated the "protocol" that let one person cause a mistake of this catastrophic magnitude?

A: The breach occurred because of both human error and technology failures. These mistakes were made in the same chain of security systems designed with redundancies.

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.

Importantly, Equifax's forensic consultants have recommended a series of improvements that are being installed over 30, 60, and 90 day periods. Equifax has 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.

Question #71 (p. 13): Is the person who failed to update the patch still employed at Equifax?

A: The individual who oversaw the team responsible for patching the relevant Apache Struts vulnerability on software supporting Equifax's online disputes portal is no longer employed by Equifax.

Question #72 (p. 13): Who was directly responsible for overseeing the employee at issue and ensuring that the security scanning system was functioning? Is this person still employed at Equifax?

A: At the time the breach was discovered, David Webb was Equifax's Chief Information Officer and Susan Mauldin was Equifax's Chief Security Officer. 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.

Question #74 (p. 13): If you had retired at the same time, but Equifax had not allowed this massive breach, how much compensation would you have received in 2016, 2017, and upon retirement?

A: Mr. Smith is unable to predict his 2017 compensation under this scenario, as the Board of Directors compensation committee tied his compensation to align with company performance and it would, therefore, be difficult to predict in light of the breach. His compensation from 2016 and retirement benefits are detailed in the Company's SEC filings.

Question #75 (p. 13): How much compensation will you be receiving instead for 2016, 2017, and upon retirement?

A: When Mr. Smith retired, he chose not take a bonus. He also volunteered to serve as an unpaid advisor for the company, helping the Board of Directors and the management team for as long as they require, for free. Ultimately, when he retired, he asked for nothing beyond what he had earned up to the date of his retirement, which he has accumulated over his career.

Question #76 (p. 13): Will you receive any compensation that is legally eligible for clawback?

A: The Company's clawback policy is outlined in the public proxy statement available on Equifax's website. The Board of Directors is currently conducting a review, which is ongoing.

Question #79 (p. 13): Will you commit to not accepting any compensation that is legally eligible for clawback?

A: Mr. Smith's compensation structure was determined by an independent committee of the Board of Directors, elected by the Company shareholders, and was aligned with the performance of the company. The Company's clawback policy is available in its proxy statement. Mr. Smith notes that there has been no restatement of the Company's financial statements nor is there any indication that such a restatement is in order.

Question #84 (p. 14): It has been reported that there was a cyber breach at Equifax in March and that Equifax hired a security firm called Mandiant to investigate the matter. Why did Equifax fail to report this breach in any SEC filing?

A: The events referred to in this question appear to reference fraud incidents experienced by TALX Corporation, a wholly-owned subsidiary of Equifax. TALX Corporation, operating under the trade name Equifax Workforce Solutions, provides human resources, payroll, tax management, and compliance services. These fraud incidents were not related to the recent cybersecurity incident (see, in pertinent part, Mandiant's supplemental report). A brief background summary of these fraud incidents follows:

- TALX experienced fraud incidents during Spring 2016 and Spring 2017.
- During the Spring of 2016, fraudsters used personal information obtained from non-Equifax sources to access employee accounts that used personally identifiable information for the user ID (e.g., Social Security numbers) and personal information for the related default PIN (e.g., the last four digits of a Social Security number or a year of birth). In response to the 2016 unauthorized access, TALX added an additional layer of authentication for the 2017 tax season so that no individual could log into the system using a default PIN containing personally identifiable information. The revised process included knowledge-based authentication ("KBA").
- During the Spring of 2017, TALX received reports of unauthorized access to individuals' W-2s contained within TALX's online platform. This incident did not involve any hacking of Equifax systems, and there was no mass exfiltration of data. While TALX was combatting these fraud cases in 2017, TALX made modifications to the KBA configuration in order to make it more difficult to pass. On a moving forward basis, TALX is continuing to modify its authentication protocol.
- As Mandiant concluded, the fraud incidents involving TALX are different from and unrelated to the recently announced cybersecurity incident.

Question #86 (p. 14): When did Equifax first learn of the May 2017 breach?

A: Please see response to question #27.

Question #87 (p. 14): When did Equifax inform the FBI of the breach?

A: Please see response to question #27.

Question #88 (p. 14): When did Equifax inform the Board of Directors of the breach?

A: Please see response to question #27.

Question #89 (p. 14): When did the Equifax executives trade their Equifax stock?

A: The Board of Directors of Equifax released a report by a Special Committee of the Board of Directors 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.

Question #90 (p. 14): When did the executives at issue express their intent to sell Equifax stock?

A: Please see response to question #89.

Question #91 (p. 14): What process did the executives have to follow in order to complete the trade?

A: Please see response to question #89.

Question #92 (p. 14): What evidence does Equifax have that suggests that the executives did not know about the breach at the time of the trade?

A: Please see response to question #89.

Question #93 (p. 14): My understanding is that Equifax's Chief Legal Officer, John Kelley, had to approve the trades at issue. Is that correct?

A: Please see response to question #89.

Questions for Mr. Richard F. Smith, Former Chairman and Chief Executive Officer of Equifax, Inc. from Senator Richard Shelby:

Question #95 (p. 15): What were the internal controls at Equifax that allowed one person's mistake to leak over 140 million American's data?

A: The breach occurred because of both human error and technology failures. These mistakes were made in the same chain of security systems designed with redundancies.

Equifax is conducting an investigation related to the incident announced on September 7, 2017 and is dedicated to resolving any issues identified as a result of that investigation. Equifax has implemented certain technological remediation steps as described in the Mandiant executive summary, which was submitted to this Committee on October 1, 2017.

Question #96 (p. 15): In your opinion, was the chain of command appropriately organized if one person's error could cause this massive 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.

Question #98 (p. 15): Did Equifax have a contingency plan in place to respond to data theft?

A: 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 ("CTC") 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.

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC.

- 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 faces numerous cyber threats every day. Its 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.

There is an ongoing root cause investigation into multiple issues, including compliance with Equifax's plans and procedure guides.

Question #99 (p. 15): Why was Equifax not taking action to prevent this type of attack in March, when it was first alerted about potential vulnerabilities?

A: 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 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. Equifax now knows 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.

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC.

On March 15, 2017, Equifax's information security department 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.

Equifax is conducting an investigation related to the incident announced on September 7, 2017 and is dedicated to resolving any issues identified as a result of that investigation.

Questions for Mr. Richard F. Smith, Former Chairman and Chief Executive Officer of Equifax, Inc. from Senator Chris Van Hollen:

Question #101 (p. 16): Federal filings show that before the breach, Equifax and the Consumer Data Industry Association lobbied on a Consumer Financial Protection Bureau rule that would prohibit forced arbitration in consumer contracts, including credit monitoring products like those Equifax offered after the breach. Please describe any lobbying activity by Equifax, its affiliates, or its agents between July 1, 2017 and October 11, 2017 (including the approval of lobbying expenditures and any meetings between lobbyists and lawmakers). In each case, please state (1) the date of the expenditure approval or meeting, as the case may be; (2) the bill, rule, or matter at issue; (3) the houses of Congress and federal agencies lobbied; (4) the individual(s) who made the decision to lobby; (5) when the individual(s) who made the decision to lobby became aware (a) of the "suspicious activity" to which you referred in your testimony and (b) that this suspicious activity may have exposed consumers' personal information; and (6) whether and when you and the current interim CEO became aware of the lobbying decision or meeting, as the case may be.

A: Please see response to question #20.

Question #102 (p. 16): Can you also list all other instances where Equifax, its affiliates lobbies against the CFPB's Mandatory arbitration rule?

A: Please see response to question #20.

Questions for Mr. Richard F. Smith, Former Chairman and Chief Executive Officer of Equifax, Inc. from Senator Elizabeth Warren:

Question #103 (p. 17): What was the precise extent of the breach?

A: As part of the incident, the attackers were able to access records across numerous tables with inconsistent schemas. The forensic investigation was able to standardize columns containing various types of sensitive information (listed below). These represent the data fields across attacker-accessed tables that were identified as potentially containing PII. The list of data elements is not exhaustive of all possible data elements in a given table, but instead represents the common PII data elements in the attacker queries.

With the foregoing in mind, the list of data elements is as follows:

- SSN
- First Name
- Last Name
- Middle Name
- Suffix
- Gender
- Address
- Address2
- City
- State
- ZIP
- Phone
- Phone2
- DL #
- DL License State
- DL Issued Date
- D.O.B.
- Canada SIN
- Passport #
- CC Number
- Exp Date
- CV2
- TaxID
- Email Address
- Full Name

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. For your reference, Equifax provided copies of the

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC.

executive summary and supplemental report to the Committee on October 1, 2017 and a copy of the final supplement to the Committee on October 6, 2017.

Question #108 (p. 17): Your press release indicates that "certain dispute documents with personal identifying information" were accessed for 182,000 U.S. customers. Exactly what kinds of documents were accessed?

A: The dispute documents accessed in this breach were documents that consumers uploaded to Equifax's online credit dispute portal. As a national credit reporting agency, Equifax has a statutory obligation to facilitate disputes between consumers and their creditors. The documents at issue were documents that consumers uploaded to Equifax in support of a credit file dispute. The documents and information contained in the documents varied by consumer, and some documents may have contained sensitive personal information. Consumers received a list of the documents, and the date those documents were uploaded, with the direct mail notifications.

Question #109 (p. 17): Were any other kinds of document or information accessed besides names, Social Security numbers, birth dates, addresses, driver's license numbers, credit card numbers, and "certain dispute documents"? If yes, what type of documents, and how many U.S. consumers were affected?

A: Please see response to Question #103.

Question #110 (p. 17): What does Equifax mean when the company says that "the incident potentially impacts" personal information? Was information merely exposed to hackers, or were hackers able to exploit and exfiltrate any personal information?

A: Please see response to Question #103, 108, and 109.

Question #112 (p. 18): Has the company identified the hackers? Is there reason to believe that they are State actors?

A: Equifax is not aware of evidence sufficient for attribution, but has shared evidence with law enforcement for the investigation of the criminal conduct.

Quesiton #113 (p. 18): How, precisely, was the personal data that was exposed to the hackers stored and protected? Was this data stored on an internet-accessible outward-facing database?

A: Please see the Mandiant executive summary, supplemental report, and final supplement. Equifax is conducting an investigation related to the incident announced on September 7, 2017 and is dedicated to resolving any issues identified as a result of that investigation. Equifax is also currently undertaking a separate assessment of its security program, which may result in additional improvements to or refinements of the existing

procedures. The Special Committee continues to review the cybersecurity incident, the Company's response to it, and all relevant policies and practices.

Question #114 (p. 18): Was the personal information of millions of Americans encrypted in any way? If not, has Equifax begun to use encryption in light of the recent breach?

A: Please see the Mandiant executive summary, supplemental report, and final supplement. Equifax is conducting an investigation related to the incident announced on September 7, 2017 and is dedicated to resolving any issues identified as a result of that investigation. Equifax has 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.

Question #115 (p. 18): Did the hackers access the data directly via the Apache Struts vulnerability, or were the hackers able to jump from the initial breached system to the corporate network to get that information? If so, how did this occur?

A: Please see the Mandiant executive summary, supplemental report, and final supplement. Equifax is conducting an investigation related to the incident announced on September 7, 2017 and is dedicated to resolving any issues identified as a result of that investigation. Equifax is also currently undertaking a separate assessment of its security program, which may result in additional improvements to or refinements of the existing procedures. The Special Committee continues to review the cybersecurity incident, the Company's response to it, and all relevant policies and practices.

Question #116 (p. 19): What steps did Equifax take to patch Apache Struts beginning in March 2017? Please provide a detailed timeline of all work on this patch from March 2017 to the present.

A: On March 8, 2017, 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, 2017 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. Equifax now knows 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, 2017 Equifax's information security department ran scans that should have identified any systems that were vulnerable to the Apache Struts issue identified by U.S.

CERT. Unfortunately, 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. Equifax's investigation into these issues is ongoing, but the Company knows that it was this unpatched vulnerability that allowed hackers to access personal identifying information.

On July 29, 2017, 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 and patched the relevant vulnerability before the web application was later brought back online.

Equifax is conducting an investigation related to the incident announced on September 7, 2017 and is dedicated to resolving any issues identified as a result of that investigation. Equifax has implemented certain technological remediation steps as described in the Mandiant executive summary, which was submitted to this Committee on October 1, 2017.

Question #117 (p. 19): Your testimony states that Equifax's security department "required that patching occur" within 48 hours. What did Equifax do to require patching?

A: Please see response to question #116.

Question #118 (p. 19): Did executives follow up with system users in the following weeks to ensure that the patching had occurred?

A: Please see response to question #116.

Question #119 (p. 19): Did Equifax monitor its systems to ensure that patching had occurred?

A: Please see response to question #116.

Question #120 (p. 19): Did Equifax do anything besides contact system users as part of its efforts to "require" patching of the Apache Struts vulnerability?

A: Please see response to question #116.

Question #121 (p. 19): What safeguards did Equifax have in place to protect against vulnerabilities in the event that all users did not immediately patch an identified weakness? What safeguards has Equifax put in place since this breach?

A: Please see response to question #33.

Question #122 (p. 19): How have Equifax's protocols and procedures for responding to an identified vulnerability changed since this 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.

Equifax has 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.

Question #123 (p.19): Which executive in the company was responsible for ensuring that this patch was successfully installed?

A: Please see responses to questions #71 and #72.

Question #124 (p. 19): Was the Apache Struts weakness the only vulnerability that was exploited by the hackers, or has Equifax identified any other weaknesses or vulnerabilities in your cybersecurity system? If so, what were these vulnerabilities and have they been resolved?

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. For your reference, Equifax provided copies of the executive summary and supplemental report to the Committee on October 1, 2017 and a copy of the final supplement to the Committee on October 6, 2017.

Equifax's internal investigation of this incident is ongoing and the Company continues to work closely with the FBI in its investigation.

Question #125 (p. 19): Has Equifax investigated why and how these scans failed to identify the continuing vulnerability? If so, what has the investigation determined?

A: Equifax is conducting an investigation related to the incident announced on September 7, 2017 and is dedicated to resolving any issues identified as a result of that investigation. Equifax has implemented certain technological remediation steps as described in the Mandiant executive summary, a supplemental report, and a final supplement. For your reference, Equifax provided copies of the executive summary and supplemental report to the Committee on October 1, 2017 and a copy of the final supplement to the Committee on October 6, 2017.

Question #127 (p. 19): Has Equifax performed a full evaluation of its security department to determine whether this and other automated security measures are fully functioning?

A: Equifax has 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.

Question #128 (p. 20): Did Equifax have safeguards in place to prevent against catastrophic consequences in the event of a failed scan? If not, has Equifax put such measures in place since the breach occurred?

A: Please see responses to questions #33 and #70.

Question #129 (p. 20): How have Equifax's protocols and procedures for running scans to determine if a vulnerability has been patched changed since the breach?

A: Please see response to question #70.

Question #130 (p. 20): Did Equifax consider notifying consumers of a potential breach of their personal information before September 7th?

A: Please see response to question #27.

Question #131 (p. 20): Why did Equifax decide not to give consumers an initial disclosure regarding the potential impacts of the breach that would have allowed them to take precautionary measures to protect themselves?

A: Please see response to question #27.

Question #132 (p. 20): More than two months after the breach, Equifax revised the estimated number of individuals impacted from 143 million to 145.5 million. Given that 40 days elapsed between the discovery of the breach and the initial announcement, how did Equifax miscount the number of affected individuals?

A: As noted in the September 7, 2017 press release, the work to determine the scope of the intrusion was substantially complete, but remained ongoing. As part of that work, Mandiant, a leading independent cybersecurity firm, was engaged to investigate this incident. Mandiant provided Equifax with an executive summary, a supplemental report, and a final supplement. For your reference, Equifax provided copies of the executive summary and supplemental report to the Committee on October 1, 2017 and a copy of the final supplement to the Committee on October 6, 2017.

In addition, Equifax issued a press release regarding the cybersecurity incident on October 2, 2017, which included the following information:

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC.

> Mandiant has completed the forensic portion of its investigation of the cybersecurity incident disclosed on September 7 to finalize the consumers potentially impacted. . . .
>
> The completed review determined that approximately 2.5 million additional U.S. consumers were potentially impacted, for a total of 145.5 million. Mandiant did not identify any evidence of additional or new attacker activity or any access to new databases or tables. Instead, this additional population of consumers was confirmed during Mandiant's completion of the remaining investigative tasks and quality assurance procedures built into the investigative process. . . .
>
> [T]he individuals identified in this update, and the unauthorized access of information, all relate to the cybersecurity incident disclosed on Sept. 7.
>
> To minimize confusion, Equifax will mail written notices to all of the additional potentially impacted U.S. consumers identified since the Sept. 7 announcement. The feature on the website that U.S. consumers may use to determine whether they may have been impacted will be updated to reflect the additional potentially impacted U.S. consumers discussed in this release by no later than October 8. . . .

Equifax's internal investigation of this incident is ongoing.

Question #133 (p. 20): Is Equifax confident in the new number, or should consumers expect another re-calculation in the future? Where did the 2.5 million new accounts come from?

A: Please see response to question #132.

Questions #134-136 (p. 20): Prior to July 29, 2017 did Equifax have a plan in place to respond to a large-scale security breach? If so, please provide a copy of this plan. If so, was this plan followed in its entirely following the July 2017 breach? If not, where did the Equifax response deviate from this plan, and why?

A: Please see response to question #98. The plans referenced in #98 are being submitted to the Committee as documents Bates numbered EFXCONG-SBC000000015 to EFXCONG-SBC000000185.

Regulatory filings show that three Equifax executives – CFO John Gamble, U.S. Information Solutions President Joseph Loughran, and Workforce Solutions President Rodolfo Ploder – sold stock in the company on August 1st and 2nd, just days after the initial discovery of the breach. At the recent hearing, you claimed that as far as you knew, these men had no knowledge of the extent of the breach, and that these sales were done as a matter of due course, even being cleared through the Chief Legal Officer. While this breach has put the financial security of hundreds of millions of Americans at risk, it is disconcerting that three executives may have decided to profit off their insider information.

Question #137 (p. 21): Were any of the three executives listed above (CFO John Gamble, U.S. Information Solutions President Joseph Loughran, and Workforce Solutions President Rodolfo Ploder) aware of the suspicious activity as of August 1st or 2nd?

A: Please see response to question #89.

In your testimony, you claimed that neither you nor anyone at the company was aware of the severity of the breach in early August. You also noted that Equifax retained the cybersecurity group at the law firm of King & Spalding, hired cybersecurity firm Mandiant to investigate the activity, and contacted the FBI on August 2, 2017.

Question #144 (p. 21): Were any of the three executives who sold Equifax stock aware of plans or the decision to take any of those three actions?

A: Please see response to question #89.

Question #146 (pp. 21-22): In response to the breach, and ostensibly to help consumers determine if their data has been hacked, Equifax created a new website, Equifaxsecurity2017.com. The New York Times reported that, after the website initially went live, consumers were unable to determine with certainty if their information was breached, reporting that the Equifax site for consumers indicated – in response to all inquiries – that personal information "may have" been compromised. As of October 10th, members of my staff were still unable to determine with certainty if their information was compromised. Why was Equifax unable to provide clarity on whether individuals' information was breached?

A: Equifax is continuously working to enhance and improve consumers' experience with the incident website. Following the initial launch of the "Am I impacted?" search tool on September 7, the Company resolved some technical issues with the search functionality. Following the completion of a forensic investigation on October 2, the Company is now able to provide a more definite impact response to U.S. consumers that take advantage of the "Am I impacted?" search tool, which can be accessed by going to the home page of this site: www.equifaxsecurity2017.com.

In addition, following completion of the forensic investigation on October 2, the Company has:

- Mailed written notices to the approximately 2.5 million additional U.S. consumers that were potentially impacted; and
- Updated the "Am I impacted?" search tool, on the website to include the entire impacted population of approximately 145.5 million U.S. consumers.

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC.

Question #147 (p. 22): Is there any way for individual consumers to determine with certainty if they were part of the breach? If this cannot be done via the website, how can they determine if this is the case?

A: Please see response to question #146.

Question #152 (p. 22): Why did Equifax's Twitter account tweet the link to a false domain not owned by Equifax several times?

A: An independent contractor mistakenly sent out the inaccurate tweets, and the company removed the tweets as soon as it learned of the error.

Question #153 (p. 22): Why did Equifax initially include a requirement that consumers consent to arbitration? Did the public outcry against the provision play any role in the decision to remove the arbitration clause?

A: Equifax has addressed confusion concerning the arbitration clauses initially included in the Terms of Use applicable to TrustedID products. Equifax never intended for these clauses to apply to this cybersecurity incident. The Company clarified that those clauses do not apply to this cybersecurity incident or to the complimentary TrustedID Premier offering. The Company clarified that the clauses will not apply to consumers who signed up before the language was removed. Equifax has updated the Terms of Use and the www.equifaxsecurity2017.com website to reflect this point.

Equifax initially included a requirement that consumers consent to arbitration in order to determine whether their data had been breached. Equifax also originally required that impacted individuals give their credit card information in order to get one free year of the company's TrustedID Premier credit monitoring and indicated that it would automatically begin billing customers if they did not cancel the subscription within a year.

Question #154 (p. 22): Does Equifax require consumers to consent to arbitration with respect to any of its other products? If so, please provide a list.

A: Please see response to Question #14.

Question #157 (p. 23): Why did Equifax initially choose to use the auto-billing model for customers?

A: Equifax has never requested consumers' credit card information when they sign up for the free credit file monitoring and identity theft protection that the company is offering to all U.S. consumers. Consumers who sign up for TrustedID Premier will not be automatically enrolled or charged after the conclusion of the complimentary year of TrustedID Premier. Following the expiration of the one year enrollment Equifax is providing to all consumers, those consumers are free to sign up for an Equifax identity monitoring product, sign up for an identity monitoring product from a competing

provider, or take no action at all. Additionally, Equifax hopes consumers will enroll in its new application that will be available in January 2018.

Question #159 (p. 23): Consumers initially were required to submit sensitive information to TrustedID in order to sign up for credit monitoring. What evaluations has Equifax done of its current data security environment to ensure that the victims of this hack do not, once again, have their information stolen?

A: Equifax has implemented certain technological remediation steps as described in the Mandiant executive summary, which was submitted to this Committee on October 1, 2017.

Moreover, Equifax has 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.

Question #161 (p. 23): How does Equifax's "credit lock" differ from a traditional credit freeze? Please explain in detail how each service works.

A: At the most basic level, a credit file lock and a security freeze do the same thing: they both help prevent creditors and other lenders from accessing your Equifax credit file, with certain exceptions. Unless a consumer gives permission or takes an action, such as removing, unlocking or lifting the freeze or lock, a lender or other creditor cannot access the consumer's Equifax credit report with a security freeze or a credit file lock in place.

Security freezes (also known as credit freezes) were created in the early 2000's, are subject to regulation by each state, and use a PIN based system for identity authentication. Credit file locks were created more recently, are mobile-enabled, and use modern identity authentication techniques, such as username and passwords and one time passcodes for better user experience.

Detailed directions for freezing or locking an Equifax credit file are set forth on the company's website. The directions are paraphrased below:

> **Lock** – To lock your Equifax credit file, enroll in TrustedID Premier. This credit file monitoring and identity theft protection product is free for one year to all U.S. consumers who enroll by January 31, 2018. Once you have finalized your activation in TrustedID Premier, visit www.trustedid.com, login and simply click the lock button. There are some exceptions where a lock may be delayed or may not be possible. Once you have finalized your activation in TrustedID Premier, visit www.trustedid.com, login, and simply click the lock button.

To unlock an Equifax credit file, once you have finalized your activation in TrustedID Premier, visit www.trustedid.com, log in and simply click the unlock button.

Freeze – An Equifax security freeze can be placed by mail, phone, or online. Equifax has waived the fee to add, lift, or permanently remove a security freeze on Equifax credit files through January 31, 2018. Any freeze activities after January 31, 2018 may be subject to the fees provided by your state of residence. The easiest and fastest way to freeze your Equifax credit file is by using Equifax's online process found at the following link: www.freeze.equifax.com. If you choose, you may also request a security freeze by calling Equifax's automated line at 1-800-685-1111. NY residents please call 1-800-349-9960. You may also submit your request in writing to:

Equifax Security Freeze
P.O. Box 105788
Atlanta, Georgia 30348

When you freeze your Equifax credit file, you will receive a 10-digit randomly generated PIN from Equifax that you will need to save and have available should you choose to temporarily lift or permanently remove the freeze in the future.

Question #162 (p. 23): Will Equifax offer consumers the opportunity to delete their data from Equifax's systems? As of your departure, was Equifax considering this option?

A: Equifax will not offer consumers the opportunity to delete their personally identifiable information or remove accurate information on a credit report, except as required by law under the Fair Credit Reporting Act ("FCRA"), 15 U.S.C §1681 et seq., or applicable state laws.

As stated in the FCRA, "the banking system is dependent upon fair and accurate credit reporting. Inaccurate credit reports directly impair the efficiency of the banking system, and unfair credit reporting methods undermine the public confidence which is essential to the continued functioning of the banking system."[1] The law further states that the purpose of FCRA is "to require consumer reporting agencies adopt reasonable procedures for meeting the needs of commerce for consumer credit, personnel, insurance, and other information in a manner which is fair and equitable to the consumer, with regard to the confidentiality, accuracy, relevancy, and proper utilization of such information in accordance with the requirements of [the FCRA]."[2]

[1] Fair Credit Reporting Act, 15 U.S.C §1681, Sec. 602(a)(1).

[2] Fair Credit Reporting Act, 15 U.S.C §1681, Sec. 602(b).

Offering consumers the "opportunity to delete their data from Equifax's systems" would directly contradict the Federal obligation placed on consumer reporting agencies ("CRAs") to ensure that credit reports are accurate. Should a consumer delete accurate data from Equifax, or from any of the other CRAs, it would result in the creation of inaccurate credit reports which "directly impair the efficiency of the banking system," as noted above by the FCRA. It could also result in consumers potentially being considered "unbanked" by a lender, therefore unfairly hindering their access to credit.

In the *General Principles for Credit Reporting*, The World Bank has further concluded:

> "Information quality is the basic building block of an effective credit reporting environment. Accuracy of data implies that such data is free of error, truthful, complete and up to date. Inaccurate data may lead to numerous problems, including unjustified loan denials or higher borrowing costs."[3]

In addition, The World Bank's International Committee on Credit Reporting also recently stated:

> "From a policy perspective, perhaps the most important role of credit reporting consists in addressing information asymmetries between creditors and borrowers in order to facilitate an efficient and cost effective credit risk assessment. Through this means, credit reporting can help achieve lower lending costs, which in competitive markets are passed on to borrowers in the form of lower cost of capital. Moreover, it can enhance access to credit for individuals and firms. Credit reporting also contributes to financial stability. For example, services offered by Credit Reporting Service Providers (CRSPs) help improve the quality of loans made by banks and other lenders through the provision of tools used to evaluate credit risk more effectively and consistently, as well as for the active management of the loan portfolio. Credit reporting also serves to discipline debtor behavior as regards the timely repayment of their financial and certain other obligations, as a good credit history facilitates access to credit and can often obviate the need for debtors to put up tangible collateral for loans."[4]

Accurate and complete data "facilitate[s] an efficient and cost effective credit risk assessment" and "contributes to financial stability." The opportunity for consumers to selectively delete accurate information from CRAs would directly prevent a critically important component of our financial system.

Under the FCRA, consumers have the right to receive a free, annual copy of their credit report and to review the accuracy of the information included on that report. In addition,

---

[3] General Principles for Credit Reporting, The World Bank, September 2011, page 2.

[4] The Role of Credit Reporting in Supporting Financial Sector Regulation and Supervision, International Committee on Credit Reporting, The World Bank, January 2016, page 5.

consumers are entitled to a free report in the event of an adverse action, such as the denial of an application for credit, insurance, or employment, based on information in the report. Further, consumers are entitled to a free, annual copy of their credit report if they are unemployed and plan to look for a job within 60 days; if the consumer is on welfare; or if a report is inaccurate because of fraud, including identity theft.

Further, under the FCRA, CRAs, and furnishers of information provided to the CRA, are responsible for correcting inaccurate or incomplete information on a credit report, and must comply with established procedures outlined in the FCRA to enable consumers to dispute information on their credit file.

Equifax complies with the above obligations under the FCRA, which support the underlying goal of ensuring a system of "fair and accurate credit reporting" for the benefit of consumers, lenders and the entire financial system.

Question #163 (p. 23): Is Equifax considering an "opt-in" regime where consumers would decide whether Equifax should have access to their sensitive personal information in the first place? As of your departure, was Equifax considering this option?

A: Equifax is not considering an "opt-in" regime.

Question #167 (p. 24): Did Equifax consider and reject other cybersecurity strategies? If so, please describe those proposals and the reasoning behind the decision to adopt the current plan.

A: Please see response to question #33.

Question #168 (p. 24): Did Equifax have a detailed breach response plan in place prior to September 2017? If so, what specific steps did this plan entail? Was this plan followed during the response to the most recent breach?

A: Please see response to questions #98.

Question #170 (p. 24): Did Equifax "lock down" all individual credentials? Was this data stored on an internet-accessible outward-facing database?

A: Please see the Mandiant executive summary, supplemental report, and final supplement. Equifax is conducting an investigation related to the incident announced on September 7, 2017 and is dedicated to resolving any issues identified as a result of that investigation.

Moreover, Equifax has 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.

Question #174 (p. 25): Was the root cause of the breach related in any way to the previous hacks that resulted in the theft of W-2 tax and salary data from Equifax in 2016, or the theft of W-2 tax data from Equifax subsidiary TALX earlier this year?

A: Please see response to question #84.

Question #186 (p. 26): As of the most recent data, how many individuals have signed up for Equifax's free credit monitoring services?

A: As of December 20, 2017, approximately 10.8 million consumers had completed registration for TrustedID Premier and approximately 4.04 million consumers had successfully enrolled.

On September 29th, barely three weeks after the public announcement of the recent breach, the Internal Revenue Service (IRS) awarded Equifax a $7.25 million sole-source contract "to verify taxpayer identity and to assist in ongoing identity verification and validations needs of the Service." Taxpayers in Massachusetts and across the country are concerned that the same company that just put their data and financial security at risk will now be responsible for preventing taxpayer fraud.

Question #191 (p. 27): Has Equifax updated its cybersecurity to ensure that it will be able to fulfill its contract with the IRS without putting taxpayers at risk? Please describe the steps taken by Equifax to boost their security and protect taxpayers.

A: Equifax has taken important steps to improve its data security infrastructure. It is further hardening its networks, changing its procedures to require "closed loop" confirmation when software patches are applied, rolling out new vulnerability detection tools, and strengthening accountability mechanisms. Equifax has implemented certain technological remediation steps as described in the Mandiant executive summary, which was submitted to this Committee on October 1, 2017. Equifax has 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.

Question #192 (p. 27): Equifax received this sole-source contract after protesting the initial award to another company. After Equifax learned of the massive data breach in late July, did Equifax alert the IRS?

A: Equifax filed the subject protest on July 7, 2017, and remained under existing contract to perform the identity verification and validation services for the IRS through September 30, 2017. Following the public announcement of the cybersecurity incident on September 7, 2017, Equifax spoke with the IRS on September 8, 2017, and has worked closely with the agency since then to answer

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC.

its questions and, at its request, securely provided impacted data for analysis. Equifax has hosted the IRS for multiple onsite security reviews since September 7, 2017 and continues to work diligently with the agency.

Question #193 (p. 27): Did Equifax considering withdrawing its protest and permitting another company to fulfill the contract in light of the recent breach exposing fundamental flaws in its cybersecurity?

A: Equifax timely submitted its bid protest in accordance with 4 C.F.R. § 21.2(a)(2). The contracting agency, as required under the Competition in Contracting Act, 31 U.S.C. § 3553(d)(4)(A), withheld authorization of performance while the bid protest was pending before GAO. Through its protest, Equifax asked GAO to review the Agency's evaluation and make an independent determination. GAO's consideration of whether the Agency conducted a fair evaluation and reasonably adhered to the terms of its solicitation remained appropriate, notwithstanding the breach. Moreover, Equifax has found no evidence of unauthorized activity on any of Equifax's core consumer and commercial credit reporting databases and remains confident in its ability to provide identity verification services to the IRS.

Question #194 (p. 27): How many other federal contracts for handling sensitive personal information are held by Equifax? What was the value of these contracts for FY2015, FY2016, and FY2017? What is the value of these contracts for FY2018? Please provide a list and a brief summary of these contracts.

A: Equifax provides products and services to a number of federal agency customers, such as the IRS, Centers for Medicare & Medicaid ("CMS"), and Social Security Administration ("SSA"). Representative services include identity verification and validation, as well as human resources, payroll, tax management, and compliance services. Equifax is in the process of collecting additional responsive contract information and plans to submit a supplemental response to these requests.

Question #195 (p. 27): Have cybersecurity breaches affected any of the data held under any of these additional contracts?

A: Equifax has shared Mandiant's executive summary with the IRS, CMS, and SSA and has confirmed that Mandiant found no evidence of any unauthorized access to the data provided by these agencies.

As Equifax has publicized, the attackers accessed certain information related to approximately 145.5 million consumers. The attackers accessed a number of tables that contained various data elements provided by consumers. For example, some of those tables contained records related to Equifax products and services, consumer disputes, and verification of consumer identities for services provided

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC.

by customers, including the IRS. Equifax has found no evidence that the attackers manipulated or deleted any of this data.

Equifax has alerted the IRS, CMS, and SSA, among other federal agency customers. Equifax has securely provided impacted data to the IRS and SSA, pursuant to their respective requests, and continues to work diligently with these agencies.

* * *

REPORT OF THE SPECIAL COMMITTEE OF

THE BOARD OF DIRECTORS OF EQUIFAX INC.

Elane B. Stock, Chair

Robert D. Daleo

G. Thomas Hough

November 1, 2017

Counsel
Wilmer Cutler Pickering Hale and Dorr LLP

REPORT OF THE SPECIAL COMMITTEE

In September 2017, the Board of Directors of Equifax Inc. formed a Special Committee of independent directors to address matters related to the cybersecurity incident disclosed by Equifax on September 7, 2017. The Special Committee was charged with conducting an independent review of the circumstances of trading in Equifax securities by certain executives following the discovery by Equifax of suspicious activity on its network and prior to the public disclosure of the incident. The Special Committee was advised by Wilmer Cutler Pickering Hale and Dorr LLP ("WilmerHale") in conducting the review, and the Special Committee directed WilmerHale during the course of the investigation. This report presents the findings of the Special Committee and the work of WilmerHale resulting from the review of the trading.

Equifax has an Insider Trading Policy applicable to all employees. Under that policy, no employee may trade in Equifax securities if he or she possesses material non-public information regarding Equifax. In addition, Equifax directors and certain senior Equifax officers may trade in Equifax securities only in specified "trading windows" and only if they first receive preclearance by the Equifax Chief Legal Officer or his designee.

Four senior officers at Equifax who are subject to this trading preclearance requirement sought and received preclearance to sell shares in Equifax securities between July 28 and August 1, 2017. Those officers are John W. Gamble, Jr. (Chief Financial Officer), Joseph M. ("Trey") Loughran, III (President, U.S. Information Solutions), Rodolfo O. ("Rudy") Ploder (President, Workforce Solutions), and Douglas G. Brandberg (Senior Vice President, Investor Relations). Equifax identified some suspicious activity on its network on the evening of Saturday, July 29, and Equifax personnel immediately began to assess the activity.

The Special Committee examined whether the trades of those officers comported with the Company's Insider Trading Policy, whether the executives had any information about the security incident when they made their trades, and whether preclearance was appropriately obtained.[1]

For the reasons set out below, the Special Committee has determined that none of the four executives had knowledge of the incident when their trades were made, that preclearance for the four trades was appropriately obtained, that each of the four trades at issue comported with Company policy, and that none of the four executives engaged in insider trading.

METHODOLOGY

The Special Committee's review examined the circumstances under which Equifax identified suspicious activity on its network, and the review was designed to pinpoint the date on

[1] Initially, the Special Committee focused on the three officers of Equifax (Messrs. Gamble, Loughran, and Ploder) who sold shares during the period under review and who are Section 16 officers of the Company, *i.e.*, covered by Rule 16a-1(f) under Section 16 of the Securities Exchange Act on 1934. The Committee thereafter determined to expand the review to cover all officers of the company – whether covered by Section 16 or not – who required pre-clearance for trading in Equifax shares under the Company's Insider Trading Policy and who sold shares during the relevant period. This change led to the inclusion of Mr. Brandberg in the review.

which each of the four senior officers first learned of the security investigation that uncovered the breach and to determine whether any of those officers was informed of or otherwise learned of the security investigation before his trades were executed. The review also entailed analysis of the Company's Insider Trading Policy as applied to these four trades.

The Special Committee conducted an extensive review of documents and communications during the period surrounding the four officers' trading in Equifax securities. The Special Committee also conducted dozens of interviews with individuals involved in or knowledgeable about the security investigation and/or the trade preclearance process in the relevant period. Finally, the Special Committee conducted lengthy in-person interviews with each of the four senior officers who executed trades. In conducting its review, the Special Committee received full cooperation from all Equifax employees including from the four senior officers, who supplied all requested information.

Document Review. The Special Committee reviewed over 55,000 documents, comprising emails, text messages, phone logs, and other records:

- As to each of the four senior officers, the Committee reviewed all of their Equifax emails, texts, calendars, voicemails, phone logs, and electronic documents, along with all Equifax emails and texts of each of their administrative assistants, for the period July 29 through August 2, 2017.[2] For the period of August 3 through September 7 (when the incident was announced publicly), the Committee conducted a targeted review of their Equifax communications, using search terms designed to identify documents concerning the incident or trading. The Committee also reviewed relevant materials from their personal emails, texts, phone logs, and other documents. Finally, the Committee reviewed documents related to the officers' Equifax holdings and trading history.

- As to employees in the Equifax Legal Department most involved in the security investigation and/or the preclearance of the trades at issue, and for Equifax's then-Chief Security Officer, the Committee reviewed all Equifax emails, texts, voicemails, calendars, and other electronic documents for the period of July 29 through August 2. The Committee also conducted a targeted review of their emails from August 3 through September 7, using search terms to identify documents concerning trading.

- As to all Equifax employees identified as having knowledge of the security investigation on or prior to the dates of the trades at issue, the Committee conducted a targeted review of Equifax emails in the period July 29 through August 2, using search terms to identify documents concerning the four officers

[2] This period spans the Company's detection of suspicious activity on the network through the date on which the last of the senior officer's securities transactions were executed.

and, where feasible, a full review of Equifax text messages from the period July 29 through September 7.[3]

Interviews. The Special Committee conducted 62 interviews, including lengthy in-person interviews with each of the four senior officers. During those interviews, the Committee addressed the officers' trading history, documents and recollections surrounding the August 2017 trades, and knowledge of the security investigation that uncovered the breach. The Committee also interviewed, in person or telephonically, each current or former Equifax employee identified as potentially possessing knowledge of the security investigation on or before the date on which the senior officers conducted their trades. During those interviews, the Committee sought to determine whether the employee had contact with any of the four officers during that period, and if so, whether that contact included any discussion of the security investigation then underway.

FINDINGS

The Special Committee found the following concerning the trading by each of the four senior officers:

John Gamble. As is standard under the Company's Insider Trading Policy, Mr. Gamble received notification by email on Tuesday, July 25 that the trading window for Equifax share transactions by executives would open on Friday, July 28 and remain open through Monday, August 31. The email instructed Mr. Gamble and the other recipients of the notification to seek preclearance from the Legal Department for any contemplated securities transactions during the window, and that preclearance, if given, would be valid for two days.

Mr. Gamble traveled to Utah with his wife on July 28 on non-Equifax business. On July 31, while in Utah, Mr. Gamble sent an email to the Legal Department requesting preclearance to sell 6,500 shares of Equifax stock (approximately 13.4% of his holdings at the time). Mr. Gamble's Equifax share grants had recently started to vest, and he had previously discussed with his financial adviser his goals to diversify his assets and to pay for an ongoing home renovation. Mr. Gamble's request to trade was approved via email on July 31, and the trade was executed on August 1.

Nine days after Mr. Gamble's trade, on August 10, during a management offsite meeting, Mr. Gamble first learned of the existence of a security incident at Equifax that was under investigation. Mr. Gamble received a more detailed briefing the following week, on August 17, and received additional details of the incident on August 22, during a Senior Leadership Team meeting.

---

[3] On August 15, 2017, the Equifax Legal Department imposed a trading blackout on all company personnel identified as aware of the breach as of that date. The Special Committee used the recipient list for the August 15 blackout notice to isolate the initial population of Equifax employees whose documents and communications should be reviewed. To the extent additional individuals were identified as potentially knowledgeable about the breach investigation during the Committee's review, their emails and texts were subject the same process, and those persons were interviewed.

The Special Committee concluded that Mr. Gamble did not have any knowledge of the security incident when he sought preclearance to trade on July 31 or when he executed his cleared trades on August 1. The Special Committee further concluded that Mr. Gamble fully complied with Company policy and did not engage in insider trading.

Trey Loughran: As is standard under the Company's Insider Trading Policy, Mr. Loughran received notification by email on Tuesday, July 25 that the trading window for Equifax share transactions by executives would open on Friday, July 28 and remain open through Monday, August 31. The email instructed Mr. Loughran and the other recipients of the notification to seek preclearance from the Legal Department for any contemplated securities transactions during the window, and that preclearance, if given, would be valid for two days.

Mr. Loughran sent an email to the Legal Department requesting preclearance to sell Equifax securities on July 28, 2017, one day before suspicious activity on the network was identified. On July 31, in response to a request from the Legal Department for greater specificity regarding the number and type of shares he wanted to sell, Mr. Loughran clarified that his request was to sell 4,000 shares (approximately 9.4% of his holdings at the time). Mr. Loughran's request for preclearance was approved on July 31, and the sale occurred on August 1. Mr. Loughran's sale of Equifax securities was consistent with previous sales he had made and was part of an effort to diversify his holdings.

Mr. Loughran first learned, at a general level, that a security issue was being investigated in a series of texts, emails, and phone calls he exchanged with members of the Equifax Legal Department on August 13 and 15. Mr. Loughran learned details of the breach on August 22, when he attended the Senior Leadership Team meeting referenced above.

The Special Committee concluded that Mr. Loughran did not have any knowledge of the security incident when he sought preclearance to trade on July 28 or when he executed his cleared trades on August 1. The Special Committee further concluded that Mr. Loughran fully complied with Company policy and did not engage in insider trading.

Rudy Ploder: As is standard under the Company's Insider Trading Policy, Mr. Ploder received notification by email on Tuesday, July 25 that the trading window for Equifax share transactions by executives would open on Friday, July 28 and remain open through Monday, August 31. The email instructed Mr. Ploder and the other recipients of the notification to seek preclearance from the Legal Department for any contemplated securities transactions during the window, and that preclearance, if given, would be valid for two days.

Mr. Ploder sent an email to the Legal Department requesting preclearance to sell Equifax securities on August 1. Preclearance was granted that same day, and his trade executed on August 2. Mr. Ploder sold 1,719 shares (approximately 3.8% of his holdings at the time). Mr. Ploder's trade was motivated by, among other things, a need to meet costs associated with a business-related move to St. Louis and was consistent with his previous sales of Equifax shares.

Mr. Ploder learned of the security incident on August 22, 2017, when he participated in the Senior Leadership Team meeting referenced above.

The Special Committee concluded that Mr. Ploder did not have any knowledge of the security incident when he sought preclearance to trade on August 1 or when he executed his cleared trades on August 2. The Special Committee further concluded that Mr. Ploder fully complied with Company policy and did not engage in insider trading.

Douglas Brandberg: As is standard under the Company's Insider Trading Policy, Mr. Brandberg received notification by email on Tuesday, July 25 that the trading window for Equifax share transactions by executives would open on Friday, July 28 and remain open through Monday, August 31. The email instructed Mr. Brandberg and the other recipients of the notification to seek preclearance from the Legal Department for any contemplated securities transactions during the window, and that preclearance, if given, would be valid for two days.

Mr. Brandberg sent an email to the Legal Department requesting preclearance to sell Equifax securities on August 1, 2017. Preclearance was granted on August 1, and his trade was executed on August 2. Mr. Brandberg sold 1,724 shares. Mr. Brandberg's sale of Equifax securities was consistent with his previous practice of selling shares as they vested; his sale was driven by family expenses.

Mr. Brandberg first learned that a security issue was being investigated on approximately August 14, and learned details of the security incident on August 22, when he attended the Senior Leadership Team meeting referenced above.

The Special Committee concluded that Mr. Brandberg did not have any knowledge of the security incident when he sought preclearance to trade on August 1 or when he executed his cleared trades on August 2. The Special Committee further concluded that Mr. Brandberg fully complied with Company policy and did not engage in insider trading.

The Application of the Insider Trading Policy. Messrs. Gamble, Loughran, Ploder, and Brandberg each sought and received clearance from the appropriate Legal Department personnel prior to trading. Based on its review, the Committee has concluded that neither Equifax's Chief Legal Officer nor his designated preclearance officer had reason to believe that Messrs. Gamble, Loughran, Ploder, or Brandberg had knowledge of the security incident's existence as of the date of their preclearance requests or the date of their trades. Accordingly, the Special Committee has concluded that the preclearance authorization obtained by Messrs. Gamble, Loughran, Ploder, and Brandberg was within the authority permitted under the policy.

* * *

The Special Committee continues to review the cybersecurity incident, the Company's response to it, and all relevant policies and practices.

ADDITIONAL MATERIAL SUPPLIED FOR THE RECORD

LETTER SUBMITTED BY THE CREDIT UNION NATIONAL ASSOCIATION

Credit Union National Association
CUNA

Jim Nussle
President & CEO

Phone: 202-508-6745
jnussle@cuna.coop

601 Pennsylvania Avenue NW
South Building, Suite 600
Washington, D.C. 20004-2601

October 4, 2017

The Honorable Mike Crapo
Chairman
Senate Banking, Housing and Urban Affairs
Committee
Washington, DC 20510

The Honorable Sherrod Brown
Ranking Member
Senate Banking, Housing and Urban Affairs
Committee
Washington, DC 20510

Dear Chairman Crapo and Ranking Member Brown:

On behalf of America's credit unions, thank you for holding the hearing titled, "An Examination of the Equifax Cybersecurity Breach." The Credit Union National Association (CUNA) represents America's credit unions and their 110 million members.

The massive Equifax data breach has put more than 143 million American consumers at risk by exposing consumers' most personal information along with hundreds of thousands of credit card numbers. Stolen information includes personally identifiable information (PII), including Social Security numbers, birth dates, and driver's license numbers and payment card data including credit and debit card numbers.

CUNA has voiced its intent to file a lawsuit to protect credit unions and their members from harm resulting from the Equifax data breach. The breach has harmed and will harm credit unions and their members. Hackers had access to highly sensitive PII and payment card data for months exposing credit unions to damages in replacing members' payment cards, covering fraudulent purchases and taking protective measures to reduce risk of identity theft and loan fraud and assuming financial responsibility for various types of fraudulent activity related to stolen identities and misuse of PII and payment card data.

Equifax and the other two credit reporting agencies (CRAs) are integral to the loan underwriting process facilitating the extension of credit by credit unions, banks and others to American consumers. Credit unions, banks and others provide Equifax with their members' and customers' information so that Equifax may use its expertise to aggregate, process and analyze information so that it can be marketed to the financial services industry and to consumers directly. Credit unions and banks also purchase information from Equifax and other CRAs for the purposes of analyzing credit worthiness and financial condition of consumers and provide purchase information to Equifax and the other CRAs .

We encourage you and your colleagues to ensure that consumers impacted have been properly notified and that Equifax has taken all measures to ensure that consumers are not at further risk. On behalf of America's credit unions, thank you for holding today's hearing. We look forward to continuing to work with you on this important issue.

Sincerely,

Jim Nussle
President & CEO

EQUIFAX, INC., "INSIDER TRADING POLICY"

EQUIFAX

EQUIFAX CONFIDENTIAL

CORPORATE POLICIES DOCUMENT

INSIDER TRADING POLICY

POLICY NUMBER: EQ-Legal-002
POLICY MANAGER: Lisa Stockard, Assistant Secretary
SLT MEMBER: J. Kelley, Corporate Vice President, Chief Legal Officer and Corporate Secretary
LAST MODIFIED: July 2017
DATE OF LAST SLT MEMBER REVIEW: July 2017
BOARD APPROVAL REQUIRED: No

POLICY OVERVIEW

This Policy concerns the handling of material, non-public information relating to Equifax Inc. ("Equifax," the "Company," or "we") or other companies with which we deal and with the buying and selling of stock and other securities of Equifax and other companies. This Policy is designed to further enhance our corporate compliance program to prevent inadvertent insider trading or allegations of insider trading, and to protect our reputation for integrity and ethical conduct. This Policy supplements the restrictions set forth in the Equifax Code of Ethics and Business Conduct (the "Code of Ethics").

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC.

TABLE OF CONTENTS

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000002

I. EMPLOYEE GROUPS; SUMMARY OF RESTRICTIONS

For purposes of this Policy, each Equifax employee, officer and director will be categorized into one of three groups as described below. Different restrictions described in this Policy apply to each group. The Office of Corporate Secretary, under the direction of the Chief Legal Officer ("CLO"), will work with the Company's management team to determine the appropriate group for each employee, and each employee will be notified by the Office of Corporate Secretary if he or she has been placed into or removed from Group Two or Group Three.

You should read this entire Policy. However, for your convenience, the following is a summary of the restrictions that apply to each group under this Policy:

- Group One - The majority of our employees are in Group One. Members of Group One are required to comply with the prohibitions on (i) trading in securities while in possession of material, nonpublic information ("insider trading"), as described in Section II of this Policy and in the Code of Ethics, and (ii) disclosing material nonpublic information to others ("tipping"), as described in Section III of this Policy and in the Code of Ethics.

- Group Two - Certain of our officers and other employees with regular access to material, non-public information are in Group Two. In addition to the general prohibitions against insider trading and tipping, members of Group Two may only purchase or sell Equifax securities during the trading windows described in Section IV of this Policy.

- Group Three - Members of our board of directors and certain senior officers are in Group Three. Members of Group Three are subject to the same restrictions as apply to Group Two. In addition, members of Group Three are required to pre-clear most transactions with the CLO (or his or her designee), as described in Section V of this Policy and will be notified separately of certain other trading restrictions and reporting requirements imposed on them by the federal securities laws and the rules and regulations of the United States Securities and Exchange Commission ("SEC").

A list of the members of Groups Two and Three will be maintained by the Office of Corporate Secretary and distributed internally and externally as appropriate.

In addition, regardless of group affiliation, any employee, officer or director of Equifax may be temporarily prohibited from buying or selling Equifax securities during special blackout periods. These special blackout periods are described in Section IV of this Policy.

II. INSIDER TRADING PROHIBITED

General Rule. No Equifax employee, officer or director may purchase or sell Equifax securities while he or she is in possession of material, nonpublic information relating to Equifax. This restriction does not apply to certain "Permitted Transfers," which are discussed in Section VI of this Policy.

Employees, Officers, Directors and Related Parties. This Policy applies to all employees, officers and directors of Equifax and its subsidiaries. Each provision of this Policy that applies to an employee, officer and director also applies to:

- Such individual's family members and other persons with whom he/she shares a household;
- family members or other persons who principally rely on the employee, officer or director for their financial support, regardless of where those persons reside; and
- any entity (a) over which the employee, officer or director has control or influence with respect to a transaction in securities (e.g., a trustee of a trust or an executor of an estate) or (b) in which

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000003

he/she has a material financial interest (for example, a trust of which an employee is a beneficiary).

Likewise, when we refer to "you" in this Policy, we also mean each of the persons and entities listed above with respect to you. Because the persons and entities listed above are covered by this Policy, you will be responsible for their transactions in Equifax securities and, in order to maintain your compliance with this Policy, you should ensure that they do not purchase or sell Equifax securities without your clearance.

Other Persons. It may be appropriate, in some circumstances, for persons who are not employed by Equifax (in addition to those listed above) to be subject to the same restrictions as the Company's employees and other "insiders." If you are aware of a situation in which a consultant, advisor or other person not employed by Equifax will have access to material, nonpublic information about the Company, you should bring this situation to the attention of the Office of Corporate Secretary, which will make appropriate arrangements to protect the Company.

Material, Nonpublic Information.

Material. Information is considered "material" if:

- a reasonable investor would consider it important in making a decision of whether to buy, sell or hold the security;
- a reasonable investor would view the information as significantly altering the total mix of information in the marketplace about the company that issued the security; or
- the information could reasonably be expected to have a substantial effect on the price of the security.

Nonpublic. Information is nonpublic until it has been "publicly disclosed," meaning that it:

- is published in such a way as to provide broad, non-exclusionary distribution of the information to the public; and
- has been in the public domain for a sufficient period of time to be absorbed by the market and reflected in the price of the related securities.

Examples of public disclosure include the issuance of a press release or the filing of an appropriate report with the SEC. Information is generally considered to be "nonpublic" until the expiration of a period of one full trading day after the information is released to the general public. However, this period varies depending on the type of information released, the market's expectations relating to the subject matter of the release, and the market's reaction after the information is released.

Examples of material, nonpublic information might include information about:

- the Company's financial or operating results, whether for completed periods or relating to expectations for future periods (including changes in previously-released earnings estimates or guidance and variances from analysts' consensus estimates);
- a material impairment or change in the value of the Company's assets;
- substantive discussions regarding a significant merger, acquisition, joint venture or disposition of significant assets;
- changes in top management;
- gain or loss of a significant customer;
- introduction of a significant new product or service;

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000004

- significant adverse accounting developments;
- changes in dividend policies or declaration of a stock split;
- the Company's entry into or termination of any significant contract;
- the filing of significant litigation or significant claims against the Company, developments (including settlements) in significant pending litigation, or other significant contingent liabilities affecting the Company;
- a potential enforcement action involving material penalties or a material regulatory development;
- a material security breach or other material disruption of the Company's information technology infrastructure;
- the Company's plans relating to its capital structure or outstanding securities, including issuances or repurchases of common stock or debt securities, and information about possible changes in the Company's credit ratings; and
- any other events that may require the filing of a Current Report on Form 8-K with the SEC.

Information may be material whether it is favorable or unfavorable to the Company. The list of examples provided above is merely illustrative, and there are many other types of information and events that may be material at any particular time, depending on the circumstances. Where there is any possibility that an item may be considered "material," you should treat it as such and you should confer with the Office of Corporate Secretary if you would like to review any specific situation.

Other Companies. While this Policy prohibits trading in Equifax securities while you are in possession of material, nonpublic information about Equifax, it also prohibits trading in securities of any other company about which you learn material, nonpublic information in the course of performing your duties for Equifax. For example, you may be involved in a transaction in which Equifax expects to enter into (or terminate) a substantial business relationship with another company (such as a publicly-traded customer or vendor), or acquire another company, buy a substantial amount of its stock or enter into a joint venture with the company. Even though the size of the transaction may be immaterial to Equifax, it may be material to the other company. This Policy prohibits you from trading in the securities of that company while aware of this material, nonpublic information or from tipping others regarding the information. In addition, please remember that Code of Ethics prohibit you from engaging in outside interests that represent a conflict of interest with your obligations to Equifax.

Securities; All Transactions. This Policy prohibits certain transactions in the "securities" of Equifax. Although it is usually the case that the information you gain will be material with respect to Equifax common stock, any securities that Equifax issues, such as debt securities or preferred stock, are also subject to this Policy. This Policy also applies to stock options and other derivatives related to Equifax securities, as discussed below, as well as Equifax Inc. 401(k) Plan transactions involving Equifax common stock. Purchases and sales of Equifax securities are subject to the insider trading laws and the provisions of this Policy, whether they are executed in the public markets or in private transactions, and whether you execute the transaction directly or indirectly through another person or entity.

Short-term Investments. We expect our employees, officers and directors to refrain from speculative transactions that are designed to result in profit based on short-term fluctuations in the price of our securities. If you do purchase Equifax securities, we strongly encourage you to do so with the expectation of owning those securities for an extended period of time — at a minimum, for six months. We recognize, of course, that your personal circumstances may change due to unforeseen events, in which case you may be forced to more quickly liquidate Equifax securities that you originally purchased with the intent of holding as a long-term investment. In addition, members of Group Three are subject to limitations on purchases and sales within a six-month period pursuant to Section 16(b) of the Exchange Act.

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000005

Short Sales. A "short sale" is (i) a transaction involving securities that the seller does not own at the time of sale or (ii) a transaction involving securities that are owned by the seller at the time of sale, but where the securities will not be delivered against such sale within 20 days thereafter or deposited in the mails or other usual channels of transportation within five days thereafter. Selling securities "short" is consistent with an expectation that the price of the securities will decline in the near future and is often speculative in nature. Short selling may arouse suspicion in the eyes of the SEC that the person was trading on the basis of inside information, particularly when the trading occurs before a major company announcement or event. Accordingly, our employees, officers and directors are prohibited from engaging in "short sales" of Equifax securities or in any other transaction involving Equifax securities that is entered into with the expectation of, or that will benefit from, a decline in the price of Equifax's securities.

Derivative Securities; Hedging. Derivative securities are securities contracts or arrangements whose value varies in relation to the price of Equifax securities. For example, derivative securities would include exchange-traded put or call options, as well as individually arranged derivative transactions. Many forms of derivatives are speculative in nature (meaning that their value fluctuates based on short-term changes in the price of Equifax securities), and the purchase or sale of such derivatives by Equifax employees, officers or directors could motivate them to take actions that are in conflict with the long-term interests of other shareholders and could also cause the appearance of misuse of inside information. Certain forms of hedging or monetization transactions, such as zero-cost collars and forward sale contracts, allow an individual to lock in much of the value of his or her stock holdings, often in exchange for all or part of the potential for upside appreciation in the stock. Such hedging and monetization transactions allow the individual to continue to own the covered securities, but without the full risks and rewards of ownership. When that occurs, the individual may no longer have the same objectives as the Company's other security holders. Accordingly, our employees, officers and directors are prohibited from purchasing or selling derivative securities, or entering into derivatives contracts or hedging and monetization transactions relating to Equifax securities. The prohibition on transactions in derivatives does not apply to stock options and other interests issued under Equifax employee benefit plans. If you have any question as to whether a particular type of arrangement or derivative transaction is permitted under this Policy, you should contact the Office of Corporate Secretary.

Pledged Securities; Margin Loans. Under typical pledge or margin arrangements, a lender or broker is entitled to sell securities which you have deposited as collateral for loans if the value of your securities falls below a specified level or in certain other circumstances. Even though you did not initiate the sale or control its timing, because it is still a sale for your benefit, you may be subject to liability under insider trading laws if such a sale is made at a time when the "window" is closed (as described below) or you are in possession of material, non-public information at the time of such a sale. If such a sale involves a member of Group Three, it can bring unwanted negative publicity to the Company and you. In addition, pledging may be used as a part of hedging strategy that would remove the full risk and rewards of stock ownership, and sever your alignment with that of Equifax's other security holders.

Group Three

Members of Group Three are prohibited from pledging Equifax securities or using Equifax securities to secure a margin loan. This Policy does not prohibit members of Group Three from holding Equifax securities in brokerage accounts, so long as any Equifax securities held in such account are explicitly excluded from any margin or pledge arrangements. Sales of Equifax securities which are held in a margin account are not exempt from insider trading laws or this Policy. Accordingly, even though utilizing accounts that exclude Equifax securities would not be subject to restrictions under this Policy, you should be extremely careful when utilizing a margin loan in a brokerage account that contains your Equifax securities.

Groups One and Two

While persons in Groups One and Two are not prohibited from pledging Equifax securities, sales of Equifax securities that you have pledged as security for a loan or which are held in a margin account are not exempt from insider trading laws or this Policy. Accordingly, even though

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000006

entering into such arrangements would not be considered a sale, and would not be subject to restrictions under this Policy, members of Groups One and Two should be extremely careful when pledging Equifax securities, utilizing a margin loan in a brokerage account or otherwise using Equifax securities as collateral for a loan.

Any sale must be made in compliance with the restrictions under this Policy that apply to you, such as trading windows and pre-clearance requirements. As a result, if you pledge your Equifax securities or use Equifax securities to secure a margin loan, you may be forced to take actions (for instance, depositing additional money or selling other securities) in order to avoid your lender or broker selling your Equifax securities at a time that would result in a violation of insider trading laws or this Policy. Similar cautions apply to any other arrangements under which you have used Equifax securities as collateral.

Members of Group Two must receive pre-clearance prior to entering into any pledge or margin arrangement involving Equifax securities to avoid an inadvertent violation of this Policy.

Safest Time for Transactions. All employees, officers and directors, whether or not subject to the trading windows or pre-clearance procedures described in this Policy, are reminded that the safest time for transactions in Equifax securities will generally be just following the trading window opens after the release by the Company of financial information relating to a completed fiscal quarter, as described in Section IV below. The appearance of improper trading may increase as the Company approaches the end of the next fiscal quarter.

III. UNAUTHORIZED DISCLOSURE OF MATERIAL, NONPUBLIC INFORMATION PROHIBITED

General Rule. No employee, officer or director may disclose material, nonpublic information about Equifax or any company with which Equifax deals to anyone outside of Equifax, unless authorized to do so.

Tipping. Under the federal securities laws, you can be held responsible not only for your own insider trading, but also for securities transactions by anyone to whom you disclose material, nonpublic information. Even if those to whom you disclose such information do not trade while aware of the information, you can be responsible for the trades of persons who received material, nonpublic information indirectly from you.

Discussing or Recommending Equifax Securities. We recognize that employee enthusiasm for Equifax and its business prospects is a vital element of our success. You should, however, use extreme caution when discussing Equifax or Equifax securities with anyone outside of Equifax. In the course of discussing Equifax or Equifax securities, accidental disclosure of material, nonpublic information can occur and can be viewed as "tipping." Likewise, recommendations of Equifax securities can also result in embarrassing situations for you or the Company if you make a recommendation at a time when there is a pending announcement of material, nonpublic information by the Company, even if you are unaware of that information.

Internet and Social Media. Consumer engagement though the Internet and social media is an important part of our business. The provisions described in this Policy about the unauthorized disclosure of material, nonpublic information and "tipping" apply equally to any statements that are made on the Internet and through social media outlets, including on our website, any form of "chat," including discussion forums and blogs, and on Facebook, Twitter, Instagram, Snapchat, Pinterest, YouTube and other outlets, by our employees, officers and directors. You should also refer to the Equifax Social Media Policy.

Authorization to Disclose Material, Nonpublic Information. We authorize only certain employees, officers and directors to make public disclosures of material, nonpublic information or to confer with persons outside the Company regarding such information (for example, our auditors, outside counsel and other advisors). Unless you are authorized to do so pursuant to the Equifax Inc. Corporate Disclosure

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000007

Policy, you should not discuss material, nonpublic information with anyone not in the Company. Even in discussions with other Equifax employees, you should consider the consequences of disclosing material, nonpublic information to them. For example, by doing so, you would preclude those persons from trading in Equifax's securities until the information is publicly disclosed. Accordingly, you should restrict the communication of material, nonpublic information to those employees, officers and directors having a need to know in order to serve Equifax's interests.

Regulation FD (Fair Disclosure). There are SEC rules and regulations banning selective disclosure of information relating to public companies. Generally, these regulations provide that when a public company (such as Equifax) discloses material, nonpublic information, it must provide broad, non-exclusionary public access to the information (for example, through press releases, conference calls or webcasts). Violations of these regulations can result in SEC enforcement actions against you and the Company, resulting in injunctions and severe monetary penalties. Regulation FD applies largely to a limited group of senior officers and the investor relations personnel who regularly communicate with securities market professionals and shareholders. Remember that no other Equifax employees, officers or directors are authorized to communicate information regarding the Company with securities market professionals, shareholders or members of the media. You should refer to the Equifax Inc. Corporate Disclosure Policy for further information about these regulations and requirements.

Non-Disclosure Agreements. Employees, officers and directors involved in transactions or other negotiations that require disclosure of material, nonpublic information with parties outside Equifax should generally have those to whom such information is being disclosed sign a non-disclosure agreement in a form approved by the Equifax legal department. The non-disclosure agreement will require that the recipient of information not disclose the information to others and require the recipient not to trade in Equifax securities while in possession of such information. You should confer with Equifax legal department whenever a non-disclosure agreement may be needed.

IV. TRADING WINDOWS

Standard Trading Windows for Groups Two and Three. If you are a member of Group Two or Three, you may only purchase or sell Equifax securities:

- during the designated trading windows described below, and
- when you are not in possession of material, nonpublic information.

Outside of the trading windows, members of Groups Two and Three may not purchase or sell Equifax securities, even if they are not personally aware of any material, nonpublic information. However, members of Groups Two and Three may engage in Permitted Transactions (described in Section VI below) outside of the trading windows.

The Office of Corporate Secretary will communicate to each member of Groups Two and Three when each trading window will open and close. It is expected that the trading window generally will open on the second trading day (assuming the first trading day is a full trading day) after our quarterly release of earnings and will close at the end of trading on the last trading day of the second month of the following quarter. However, you should not expect that the window will open on any particular date or remain open for any minimum period of time. Significant corporate developments may require changes to the schedule, including closing the window at the Company's option at any time.

Do not confuse the applicability of the trading windows with the broader prohibition on trading when you are in possession of material, nonpublic information described in Section II. Regardless of whether the trading window is open or closed, you may not trade in Equifax securities if you are in actual possession of material, nonpublic information about Equifax.

Special Blackouts. We reserve the right to impose a trading blackout from time to time on all or any group of our employees, officers or directors when, in the judgment of our CLO and other senior officers,

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000008

a blackout is warranted. During a special blackout, you will not be permitted to purchase or sell Equifax securities and you may or may not be allowed to execute Permitted Transactions (as defined below). A special blackout may also prohibit you from trading in the securities of other companies. If the CLO imposes a blackout to which you are subject, we will notify you when the blackout begins and when it ends and the securities and transactions to which it applies. Any person made aware of the existence of a special blackout should not disclose the existence of the restriction to any other person. The failure of the Company to designate a person as being subject to a special blackout will not relieve that person of the obligation to refrain from trading while aware of material, nonpublic information.

Standing Orders; Limit Orders. Purchases or sales resulting from standing orders or limit orders may result in the execution of orders without your control over the transaction or your awareness of the timing of the transaction. Even though you placed the order at a time when you were permitted to enter into transactions, you must be certain that this type of order will not be executed when you are in possession of material, nonpublic information about the Company or during a blackout period. Accordingly, any standing orders should be used only for a very brief period and with detailed instructions to the broker who will execute the transaction. Standing orders under an approved Rule 10b5-1 Trading Plan, described below, will not be subject to these limitations.

V. PRE-CLEARANCE OF TRANSACTIONS

General. Before purchasing or selling Equifax securities, members of Group Three must obtain clearance of the transaction from the CLO (or his or her designee). This clearance must be obtained **before** you place the order for, or otherwise initiate, any transaction in Equifax securities. Two business days' advance written notice is requested for a proposed transaction. Any pre-clearance that you obtain will be valid for a transaction executed within two business days, unless either the pre-clearance is granted for a shorter or longer period or you learn of material, nonpublic information during that time. Whether or not your request for pre-clearance is granted, you must not inform anyone else of the results of your request.

Do not confuse pre-clearance of transactions with the broader prohibition on trading when you are in possession of material, nonpublic information described in Section II. Regardless of whether you have received pre-clearance for a transaction or whether a trading window is open or closed, you may not trade in Equifax securities if you are in actual possession of material, nonpublic information about Equifax and your compliance with insider trading laws remains solely your responsibility.

Permitted Transactions. Members of Group Three are not required to receive pre-clearance prior to entering into any Permitted Transaction, except they are required to do so before exercising any stock options or making any gifts of Equifax securities.

VI. PERMITTED TRANSACTIONS

The following are "Permitted Transactions":

- acceptance or receipt of a stock option, shares of restricted stock or similar grants of securities under one of Equifax's equity-based benefit plans (including elections to acquire stock options or securities in lieu of other compensation) or the cancellation or forfeiture of options, restricted shares or securities pursuant to Equifax's benefit plans;
- election to participate in, cease participation in or purchase securities under an Equifax employee stock purchase plan or dividend reinvestment plan, if such a plan is in effect (see "Employee Benefit Plan Transactions" below);
- earning or vesting of stock options or shares of restricted stock and any related stock withholding;

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000009

- exercise of stock options issued under Equifax plans in a cash exercise, a stock-for-stock exercise or a net share exercise, payment of the exercise price in shares of already-owned stock and any related stock withholding transactions, **but not** (i) the sale of any stock acquired in the option exercise, (ii) a "cashless exercise" in which shares are sold in the market, or (iii) the use of proceeds from the sale of any such shares to exercise additional options (see "Employee Benefit Plan Transactions" below);
- transferring securities to an entity that does not involve a change in the beneficial ownership of the securities, for example, to an inter vivos trust of which you are the sole beneficiary during your lifetime (see "Transactions in Which There is No Change in Beneficial Ownership" below);
- making payroll contributions to and receiving matching Company contributions in the Equifax Inc. 401(k) Plan, deferred compensation plan or any similar plan, **but not** (i) intraplan transfers involving any Equifax securities nor (ii) a change in "investment direction" under such plan to increase or decrease your percentage investment contribution allocated to Equifax securities;
- bona fide gifts of securities, **but not** where you are delivering the Equifax securities in payment of a previous commitment to make a cash gift or where the Equifax securities are being delivered in payment of any other obligations (see "Gifts of Equifax Securities" below);
- execution of a transaction pursuant to a contract, instruction or plan described in Securities Exchange Act Rule 10b5-1 (called a "Trading Plan"), as discussed below (see "Trading Plans" below); or
- any other transaction designated by the Board of Directors or any Board committee or senior management, with reference to this Policy, as a Permitted Transaction.

Pre-Disclosure of Undisclosed Material, Nonpublic Information. You may not enter into any Permitted Transaction unless you have disclosed any material, nonpublic information of which you are aware to the CLO (or his or her designee); provided, that members of Group Three must disclose any such information directly to the CLO before any transaction listed qualifies as a Permitted Transaction. This ensures that Equifax is fully aware of any material information affecting any security before you enter into a transaction involving Equifax securities.

Employee Benefit Plan Transactions. Most of the ongoing transactions you might enter into under Equifax's equity-based benefit plans are included in the definition of Permitted Transactions. For example, although your ongoing participation in a plan may involve the regular purchase of Equifax's common stock, either directly pursuant to an investment election or indirectly through an employer matching contribution, those purchases are Permitted Transactions. ***Note, however, that the movement of balances in those plans into or out of Equifax securities or changes in your investment direction under those plans are not Permitted Transactions.*** This means that you may not make transfers or elections of Equifax securities while you are in possession of material, nonpublic information and that such transfers or elections must be made in compliance with any other restrictions under this Policy that apply to you (for instance, if you are in Group Three, such transfers or elections could only be made during an open trading window and with pre-clearance).

Transactions in employee stock options are also considered Permitted Transactions if there is no related sale on the market or to a person other than Equifax. ***Note, however, that a sale of stock following or in connection with an option exercise is not a transaction with Equifax and is, therefore, not a Permitted Transaction.*** Thus, you may engage in a cash exercise of an option as long as you retain the stock you buy in the exercise. You can also engage in stock-for-stock exercises or elect stock withholding without violating the Policy. However, it would not be a Permitted Transaction for you to exercise a stock option, sell the resulting shares and then use the proceeds from that sale to pay for the exercise of additional stock options in a same day sale. Although exercises of Equifax stock options are Permitted Transactions, members of Group Three must pre-clear all stock option exercises.

Transactions in Which There is No Change in Beneficial Ownership. Certain transactions involve merely a change in the form in which you own securities. For example, you may transfer shares of stock

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000010

to a trust if you are the only beneficiary of the trust during your lifetime. Likewise, changing the form of ownership to include a member of your household as a joint owner or as a sole owner is a Permitted Transaction since members of your household are considered the same as you for purposes of this Policy (and the shares will remain subject to the terms of this Policy).

Gifts of Equifax Securities. Bona fide gifts of Equifax securities, whether to charitable institutions or to friends and family members (including into any trust), are generally considered to be Permitted Transactions. However, if you are making the gift to satisfy a previous commitment to make a cash gift or in payment of another obligation, then the gift would not be a Permitted Transaction and the normal restrictions would be applicable. This Policy is designed to prevent employees from making gifts of stock when the gift will satisfy a previous pledge of cash or not be considered a "bona fide" gift. Although bona fide gifts of stock are Permitted Transfers, members of Group Three must pre-clear all gifts of shares.

Trading Plans. The SEC has enacted a rule (Rule 10b5-1 under the Securities Exchange Act of 1934) that provides an affirmative defense against violations of the insider trading laws if you enter into a contract, provide instructions, or adopt a written plan for a transaction in securities when you are not in possession of material, nonpublic information, even if it turns out that you had such information when the transaction is actually completed. The contract, instructions, or plan must:

- specify the amount, price and date of the transaction,
- specify an objective method for determining the amount, price and date of the transaction, or
- place the discretion for determining amount, price, and date of the transaction in another person who is not, at the time of the transaction, in possession of material, nonpublic information.

You may not exercise discretion or influence over the amount, price, and date of the transaction after entering into the arrangement. In this Policy, we refer to these arrangements as "Trading Plans." The rules regarding Trading Plans are extremely complex and must be complied with completely to be effective. You should consider consultation with your own legal advisor before proceeding with entering into any Trading Plan.

Any restrictions under this Policy that apply to you when purchasing or selling Equifax securities also apply to you when establishing a Trading Plan. Therefore, you may not establish a Trading Plan when you are in possession of material, nonpublic information about Equifax and, to the extent trading windows and special blackout periods apply to you, those restrictions must be complied with in connection with establishing a Trading Plan. The Company may from time to time adopt additional rules for the establishment and operation of Trading Plans, and you will need to comply with these rules in order to utilize a Trading Plan. In addition, members of Groups Two and Three are required to receive pre-clearance before entering into any Trading Plan. Once a Trading Plan for a member of Group Two or Three has been pre-cleared by the CLO, transactions executed pursuant to that Trading Plan do not require approval. Members of Group One are not required to pre-clear Trading Plans, but they are required to provide copies of their Trading Plans to the CLO prior to any trading is begun thereunder.

In establishing any Trading Plan, you should carefully consider the timing of your transactions under the Trading Plan. Even though transactions executed in accordance with a Trading Plan are exempt from the insider trading rules, the trades may nonetheless occur at times shortly before Equifax announces material news, and the media may not understand the nuances of trading pursuant to a Trading Plan.

VII. SANCTIONS FOR VIOLATIONS OF THIS POLICY

The SEC, the stock exchanges and plaintiffs' lawyers focus on uncovering insider trading, and use sophisticated technologies to investigate suspicious activity.

A breach of the insider trading laws could expose the insider to criminal fines of up to $5,000,000 and imprisonment of up to 20 years, in addition to civil penalties (up to three times the profits earned), and

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000011

injunctive actions. In addition, punitive damages may be imposed under applicable state laws. Securities laws also subject controlling persons to civil penalties for illegal insider trading by employees. Controlling persons include directors, officers and supervisors. These persons may be subject to fines of up to the greater of $1,000,000 or three times the profit realized or loss avoided by the insider. Accordingly, all Equifax employees must comply with this Policy and applicable securities laws and to ensure that those employees who they supervise also comply.

Inside information does not belong to any of Equifax's individual employees, officers or directors. This information is an asset of the company. For any person to use such information for personal benefit or to disclose it to others outside of the Company violates the Code of Ethics, this Policy and federal securities laws. More particularly, insider trading is a fraud against members of the investing public and against the Company. Whether or not there is any actual trading of our securities, any violation of this Policy will be grounds for discipline, up to termination of employment for cause.

VIII. ADMINISTRATION OF THIS POLICY

Administration and Review. The day-to-day administration of this Policy, including appropriate training, will be carried out by the Office of Corporate Secretary, under the direction of the CLO. If you have any questions concerning the interpretation of this Policy, you should direct your questions to the Office of Corporate Secretary (CorporateSecretary@equifax.com).

Reporting Violations. If you become aware of any violation of this Policy, you should report it immediately to the Office of Corporate Secretary.

Exemptions. An individual subject to the trading windows or special blackout periods described in Section IV may request that the CLO grant him or her a hardship exemption from those restrictions if he or she is not otherwise prohibited from trading under Section II. However, we anticipate that exemptions will be given very rarely and only in extreme circumstances.

Amendment of the Policy. This Policy may be amended from time to time in the discretion of the CLO. In such event, we will communicate to you through normal communications channels the substance of any such changes.

The ultimate responsibility for complying with this Policy and applicable laws and regulations rests with you. You should use your best judgment and consult with the CLO (or his or her designee), the Office of Corporate Secretary and your personal legal and financial advisors, as needed.

IX. ROLES AND RESPONSIBILITIES

Party	Role / Responsibility
Senior Leadership Team ("SLT")	• Promote and implement a strong culture of compliance; and • Support efforts to implement the Policy and sponsor appropriate action to align with the Policy.
Chief Legal Officer ("CLO")	• Provide pre-clearance of transactions by members of Group Three and Trading Plans for all employees, as may be required under the Policy; • Determine when a special blackout period is warranted; • Approve exceptions to the Policy; and

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000012

Party	Role / Responsibility
	• Approve amendments to the Policy.
Policy Manager	• Monitor Policy implementation; • Periodically review the Policy and propose revisions to the CLO as appropriate; and • Coordinate review and approval of the Policy and the internal communication of Policy changes.
Office of Corporate Secretary	• Oversee day-to-day administration of the Policy; • Provide legal interpretations insider trading laws and regulations; • Review proposed revisions to the Policy; • Work with Company's management team to determine the appropriate restrictions under the Policy for each employee and notify employees of placement in or removal from Groups Two or Three; • Maintain list of designated insiders and communicate updates to internal and external personnel, as necessary; • Distribute periodic reminders to designated insiders (members of Groups Two and Three) with information regarding trading windows and pre-clearance requirements; • Notify employees in connection with any special blackout period; • Provide legal guidance in the event that non-employees may have access to material, nonpublic information about the Company; • Assist in the development and maintenance of applicable training; and • Provide legal guidance with respect to investigations and permissible disciplinary actions.
Employees	• Read and comply with the Policy; • Report Policy violations and concerns to the Office of Corporate Secretary or the Policy Manager; and • Seek clarification from the Office of Corporate Secretary concerning any questions or concerns with respect to compliance with the Policy.
Non-Employee Directors	• Comply with the Policy; and • Report Policy violations and concerns to the CLO or other SLT member.

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000013

X. REFERENCES

- Equifax Code of Ethics and Business Conduct
- Equifax Inc. Corporate Disclosure Policy
- Equifax Social Media Policy

XI. REVISION HISTORY

Version #	Revision Date	Revision Comments
1.0	July 2017	Initial document creation; replaced existing policy on insider trading.

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000014

EQUIFAX, INC., "CORPORATE CRISIS MANAGEMENT PLAN, PART I"

EQUIFAX

Corporate Crisis Management Plan

Part I: Program Description

May 2017

Version 5.0

This document is not intended to be used during a crisis.

Refer to Part II -*Crisis Management Team Response Plan* for crisis response guidance.

This Document is not an Emergency Response Plan.
In Case of Fires, Injuries, Threatening Situations, or Other Emergencies:

Get to a Safe Place and Call 911

(Outside US: Contact Local Emergency Services)

Serious incidents should be reported as a potential Equifax crisis:

- Fatalities, serious injuries, or threatening situations.
- Fires, explosions or other events causing damage to a facility.
- The risk or actual occurrence of confidential data corruption, loss, theft, or compromise.
- Any incident causing the evacuation or shelter in place of personnel.
- Facility closure due to severe weather or other regional emergencies.
- The risk or actual occurrence of significant operational disruption from any cause.

Incidents that might be an Equifax crisis should be reported by calling the Equifax Security Hotline:

+1 770.740.5555

Suspected information security incidents will be reported to the Cyber Threat Center (CTC) by phoning:
+1 678-795-7106 or 1-888-257-8799 or emailing: [HYPERLINK "mailto:security.incident@equifax.com" \h]

© 2017 Equifax, Inc. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC.

Equifax's first priority is to protect the health and safety of people.

Once actions are underway to protect people, the action lists found in the ***Corporate Crisis Management Plan - Part II - Crisis Management Team Response Plan*** should be used to guide the overall Equifax response. **Corporate Crisis Management Plan - Executive Summary**

This corporate Crisis Management Plan is a strategic document created for Equifax's senior leadership. It provides detailed strategic response guidance for Equifax's executives to use when managing a significant incident. The plan establishes a structure and a process for integrating executive, managerial and operational resources. Finally, it provides a framework to facilitate efficient and timely collaboration between:

- Executive leaders
- Department heads and their teams
- Functional leaders and their organizations
- Subject matter experts

The plan defines and integrates all Equifax resources and supporting plans needed for effective crisis response, including:

- Emergency response
- People support
- Business continuity
- Crisis communications
- IT disaster recovery
- Card Brand notification
- All other Equifax-specific response plans

The plan mandates a crisis management "CMT Coordinator," who oversees crisis management planning, verifies the response processes defined in the plans, and audits the effectiveness of the entire response organization.

The plan is specifically intended, during a declared crisis, to:

- Take all steps needed to protect the safety/well-being of Equifax personnel and others in all Equifax facilities.
- Provide a framework for full or partial activation of broader response organizations.
- Protect the reputation, assets, mission and survivability of Equifax.

© 2017 Equifax, Inc. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC.

- Manage the effective recovery of infrastructure (systems, buildings).
- Verify continued regulatory and legal compliance.

© 2017 Equifax, Inc. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC.

The plan defines an organization with the supporting tools, equipment and processes to effectively respond to any type of serious or catastrophic incident, for example:

- Operational issues such as office/data center emergencies.
- Any situation that attracts the attention of the media and the public and could damage the reputation of Equifax.
- Kidnapping, terrorism or other serious crimes.
- Natural disasters such as hurricanes, earthquakes, or flooding.
- Public health disasters, epidemics or pandemics.
- Financial crises, such as market-related situations, a major decline in Equifax's stock price, earnings, or fraud.
- Informational crises, such as a loss of proprietary and confidential information, tampering with computer records, security incident or loss of IT infrastructure.
- Legal issues, such as the indictment or arrest of a senior executive.
- Political/Civil unrest impacting business operations or personnel.
- Loss of the use of major offices /data centers for any other reason.
- Untimely death or reported illness of a member of the executive team.
- Data breach of PCI associated data.

This plan is divided into three parts.

- The first section, **Part I: Equifax Crisis Management Plan - Program Description,** consists of Sections A through E, and is designed to:
  - Document how Equifax has agreed to prepare for, monitor and respond to a significant incident.
  - Provide a document to improve CMT members' awareness and capabilities.
  - Provide a benchmark with which to evaluate performance during an exercise or actual crisis.
- The second section, **Part II: Equifax Crisis Management Plan: Crisis Management Team Response Plan** consists of a list of strategic considerations and potential actions for Equifax's leadership, organized by function.
- The third section, **Part III: Equifax Crisis Management Plan - Appendices,** consists of supporting plans for each function and business unit, along with activation and notification procedures.

Finally, the plan includes policy, principles, scope, purpose and definition statements to help align crisis response with Equifax culture and provides guidance for principle-based decision making. It establishes authority levels and defines roles and responsibilities for executives and their organizations. Operational guidance, facilities, equipment, training and maintenance requirements are described at a high level. A supporting organization is clearly defined, and command and control protocols are established so that Equifax's leadership can quickly activate a reliable, trained and integrated response organization during the stressful and confusing events that accompany any catastrophic incident

© 2017 Equifax, Inc. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC.

Equifax Crisis Management Plan

Part I: Program Description

Table of Contents

© 2017 Equifax, Inc. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC.

NOTE: References to material outside this plan are in ***bold italic.***

© 2017 Equifax, Inc. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC.

I. Crisis Management Policy & Principles

A. Crisis Management Policy

The Equifax Company headquartered in Atlanta GA, is a global leader in consumer, commercial and workforce information solutions, providing businesses of all sizes and consumers with information they can trust. Equifax organizes and assimilates data on more than 500 million consumers and 81 million businesses worldwide, and uses advanced analytics and proprietary technology to create and deliver customized insights that enrich both the performance of businesses and the lives of consumers. Equifax operates or has investments in 17 countries and is a member of S&P 500 Index.

It is Equifax's policy to operate its businesses safely, and to be prepared to effectively respond to a crisis. The crisis management program is managed via the business continuity organization, with a mission to maximize Equifax's resiliency in the event of a disaster or significant business interruption. The overall program seeks to:

- Protect the well-being of personnel, clients and visitors.
- Protect Equifax information and facilities.
- Ensure timeliness, availability, and usability of data at time of business disruption.
- Protect against potential threats (man-made or natural).

With this mission in mind, senior Equifax management is responsible for the development, maintenance, and implementation of effective crisis management plans, processes and organizations. In furtherance of this mission, Equifax has adopted this program to train its people in crisis management. Equifax maintains a Crisis Management Team (CMT), as defined in this plan, to manage incidents that are declared a crisis.

The CMT will act based first on the concern for the welfare of all people including personnel, clients, visitors, emergency responders and community members. The secondary concern is for the protection of our assets, preservation of our ability to operate and serve our clients, maintenance of a strong Equifax reputation and ultimately the preservation of shareholder value.

B. Crisis Management Principles

If an Equifax crisis occurs, Equifax will respond using the following principles:

- Place the highest priority on Life Safety – the welfare of all people including personnel, clients, visitors, emergency responders and community members.
- Protect our assets and preserve our ability to operate and supply our customers.
- Maintain a strong Equifax reputation through ethically and socially aware behaviors that ultimately preserve shareholder value.
  - Comply with all laws, rules and regulations applicable to its operations and the incident.
  - Make public disclosures that are full, fair, accurate, timely and understandable regarding the effects of the crisis on Equifax facilities, personnel, clients and operations.
  - Make decisions and take actions that are consistent with Equifax's core values.
  - Consider all stakeholders in its actions – and as appropriate, communicate to them in a timely way and using normal channels to the extent possible.
  - During a crisis, make crisis response a priority over other needs, specifically the deployment of resources, e.g., personnel and equipment.

© 2017 Equifax, Inc. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000022

C. Crisis Management Plan Scope

Equifax maintains a Crisis Management Plan (CMP) for its CMT to use to respond to crises involving its assets, businesses, and reputation. This plan is global in scope. **The CMT is prepared to assemble personnel and begin implementing actions promptly, even as the severity of an incident is being confirmed.**

The CMP is organized in three parts:

- Part I – Program Description (this document)
- Part II – CMT Response Plan
- Part III – Regional Crisis Action Team Plans

This structure is intended to facilitate a clear and efficient crisis response by separating the reference materials needed during a response to a crisis event from administrative elements of the program. Collectively, these two parts provide a framework, organization and operating concepts for crisis response, applicable to the entire global organization, by providing response command and control, resource support, and strategic direction from Equifax leadership.

The CMP is designed to complement, not supplant, existing emergency response, disaster recovery, business continuity and crisis communications plans. It is designed to coordinate the responses of corporate and operational organizations to ensure issues and concerns of internal and external stakeholders are adequately assessed and addressed.

D. Crisis Management Plan Purpose

The ultimate purpose of the CMP is to create a process that minimizes the negative effects of a crisis through active and efficient management of the event. The bullets below describe how this will happen.

- Equifax plans in advance for various types of crises that may occur.
- A crisis management organization and responsibilities are defined, maintaining the integrity of Equifax's line organizations.
- The consequences of crises on both internal and external stakeholders are adequately assessed, and appropriate Equifax resources are coordinated and directed to a crisis.
- Early in a crisis, rapid, factual, coordinated communications are established and maintained with Equifax's internal and external audiences, with special emphasis on personnel.
- Actions are taken to ensure Equifax meets applicable regulations, guidelines and public expectations.

E. Audience

This document is to be used by the CMT and those departments and teams that may support them as defined in **Section II**.

© 2017 Equifax, Inc. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000023

F. Definitions

Corporate Crisis

A corporate crisis is an unplanned event related to Equifax's business that has the potential to:

- Present a significant threat to human health, safety or the environment.
- Cause a significant adverse effect on Equifax's reputation.
- Cause a significant disruption to Equifax's business.

Notwithstanding the definition above, a Corporate Crisis is any event identified as such by the CMT Leader or designate.

Examples of potential Equifax crises include:

- Operational issues such as office/data center emergencies.
- Any situation that attracts the attention of the media and the public and could damage the reputation of Equifax.
- Kidnapping, terrorism or other serious crimes.
- Natural disasters such as hurricanes, earthquakes, flooding
- Public health disasters, epidemics or pandemics.
- Financial crises, such as market-related situations, a major decline in Equifax's stock price or earnings, or fraud.
- Informational crises, such as a loss of proprietary and confidential information, tampering with computer records, security incident or loss of IT infrastructure.
- Legal issues, such as the indictment or arrest of a senior executive.
- Political/Civil unrest impacting business operations or personnel.
- Loss of the use of major offices /data centers for any other reason.

Corporate Incident

A corporate incident is an unplanned country-based/regional event that has the potential to cause or has caused:

- An unplanned business disruption across multiple BU/COEs
- Prolonged response/resolution requirements
- High probability of impact to multiple customers
- Media inquiries
- Life Safety issues affecting multiple workers

© 2017 Equifax, Inc. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000024

Notwithstanding the definition above, a corporate incident is any event identified as such by the CCT Leader or designate.

Examples of potential Equifax corporate incidents include:

- Extended power outage
- Extended network/telecommunications outage
- Security vulnerability
- Employee Safety (inclement weather)
- Local political/civil unrest impacting business operations or personnel.
- Local demonstrations/transportation strikes

The CMT or CCT are activated when the CMT Leader and/or Crisis Coordinator (or designate) decides an event meets or has the potential to meet the definitions above. Further information on activation procedures is provided in **Section VI.**

© 2017 Equifax, Inc. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC.

II. Organization and Responsibilities

A. CEO Responsibilities

The **CEO** is accountable for Equifax's response to a crisis situation and manages a crisis through the CMT. The CEO is not the hands-on leader of the CMT in most cases. Rather, the CEO may act as the corporate spokesperson or address other key stakeholders as needed with support from Communications and other CMT Members. The CEO retains ultimate responsibility for the effectiveness of crisis response when managed by the CMT. The CEO may delegate leadership of the CMT as defined below.

B. CMT Leadership

1. The **Chief Legal Counsel** is the Crisis Manager that has decision authority over the CMT.
2. If the **Chief Legal Counsel** is not available to direct CMT activities, the **Chief Financial Officer** will act as Crisis Manager.
3. If none of these leaders are available, another senior executive, appointed by the CEO or active CMT members will serve as Crisis Manager.

C. Crisis Management Team Personnel

Members of the Equifax CMT are senior leaders with responsibility for one or more functions or departments. **These responsibilities are defined in Table A in Section IV**. Together, the CMT has line organization control over the entire Equifax organization worldwide. Each CMT member will manage the response to an incident through a function-specific support team called a Crisis Command Team (CCT), defined in Section F below.

CMT Members representing each role on the CMT, e.g., HR, IT, Finance, Communications will be approved by the CEO and may be from various levels of seniority. Both executive level and SVP/VP level staff will be identified for each role. Staffing of the CMT may be from either level, depending on the nature and potential effects of the specific incident. If the CMT is staffed by the executives, typically the SVP/VP level personnel will lead the CATs.

Each CMT member will have at least one alternate member identified. The alternate should be equally familiar with the CMT member's roles and responsibilities. Typically, the CMT primary member and alternate member will be activated at the beginning of a crisis, and both will remain active until the need for two shifts is determine. In the case of a one shift response, the alternate member can become part of the CAT team. In the case of a two shift response, the primary and alternate members will take turns as CMT representative as defined later in this plan.

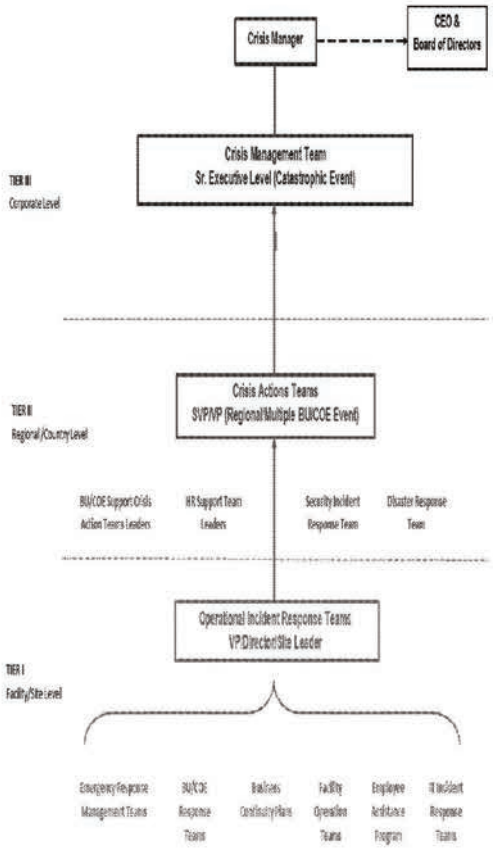
D. Overall Crisis Management Structure

The chart on the following page depicts the crisis management structure. It shows the relationship between the strategic **Crisis Management Team** shown in red, and the **Crisis Action Teams** shown in blue, along with **Operational Teams** shown in green that may be deployed during a crisis to support the Crisis Action Teams.

© 2017 Equifax, Inc. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000026

E. Overall Crisis Management Structure



© 2017 Equifax, Inc. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC.

F. Incident Response Teams

Each CMT member will require additional support to execute their CMT responsibilities. To accomplish this, the CMT is supported by Regional "Crisis Action Teams" ("CATs"), composed of SVP/VP decision maker and subject matter experts within each department. CAT members represent the specific areas of expertise, within their departments, needed to respond to a corporate incident or lower level incidents. These are the **"Managerial" teams** (blue) shown in the graphic in **Section E**.

During a corporate crisis, CMT members will activate their corresponding support Crisis Action Teams (CATs) to help set crisis response strategies and manage crisis response activities. Each CAT is comprised of the CAT leader and an alternate leader from each supporting BU/COE; contact information is listed in ***Appendix A***. Regional CAT membership is defined in each plan, respectively.

Each CMT member is responsible for ensuring viable and timely communication between themselves and their CAT support personnel. A briefing process, implemented by the CMT Coordinator will be used to ensure effective communication is maintained.

The CATs purpose is to receive information from internal and external sources, pass appropriate information to the CMT, recommend strategies and tactics to the CMT, and implement those strategies and tactics on behalf and under the direction of the CMT.

Each CAT plan lists the team members' primary responsibilities and provides a detailed checklist of specific actions to be considered during a crisis.

Administrative Support is also provided to CMT. The primary administrative duties are documenting the current status of the event for the CMT, room preparation (telephones, computers, office supplies), and arranging food/drink for extended responses.

G. Operational Teams

When the CMT is active, a CAT member will manage all active **"Operational" teams** (green) shown in **Section E** above. The Operational teams include Business Continuity, IT Recovery, Emergency Response, People Support, Crisis Communication, etc. Each CCT provides command and control protocols to ensure **Operational Plans** are executed according to the overall strategy as defined by the CMT.

NOTE: **Operational Plans** may be executed WITHOUT the CMT or CATs being activated; this is typically in less severe incidents that do not require full activation of Equifax resources. However, if an **Operational Plans** is activated, the CMT Leader or CMT Coordinator should be informed.

H. Crisis Coordinators

The Crisis Coordinators are the Equifax crisis management subject matter experts. They are responsible for ensuring that the CMT plans are maintained and that the CMT receives training and exercising according to the schedule in **Section VIII**. The Crisis Coordinator also has audit responsibility for all preparedness plans shown in **Sections E and F** above. Finally, during an exercise or actual response, the Crisis Coordinator provides process advice and guidance to the CMT using the various concepts of operations in the Crisis Coordinator's toolkit.

© 2017 Equifax, Inc. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000028

I. CMT Members and Roles

CMT roles, CMT members, CMT alternates, CAT Leaders and CAT leader alternates as of April 2017* are:

Role	Executive CMT Member	Alt Executive CMT or VP/DIR CMT Member	Alt VP/CMT Member
Crisis Manager	J. Kelley	John Gamble	
Crisis Coordinator	Susan Mauldin	Dodd Williams	Mike Douglas
Administrative Support	Mary Banks	Patricia Numprasong	Pamela Sanders
HR	Coretha Rushing	Ron Walker	Shari Lotz
IT	David Webb	Mary Hannan	Michael Ligetti
Corporate Communications	Ines Gutzmer	Marisa Salcines	Meredith Griffanti
Legal	J. Kelley	Julia Houston	Jennifer Burns
Finance	John Gamble	Ken Marshall	Nuala King
Global Operations	Andy Bodea	Tony Weeks	Scott Vogt
Safety and Security	Susan Mauldin	Greg Baker	Steven Cosby
Real Estate	Trey Briscoe	Jim McCarthy	Karen Dick
Marketing & Analytics	Trey Loughran	Aparna Shah	Anir Pradhan
GCS	Trevor Burns	Dann Adams	Assad Lazarus
Workforce Solutions	Rudy Ploder	Mike Mohr	Ellen Stanko
Corporate Development	Steven Stripe	Dustin Renn	Kelly Heape
International	John Hartman	Rob Eison	Mark Rohrwasser
USIS	Paulino Barros	Shawn Holtzclaw	Isio Nelson
Investor Relations	Jeff Dodge		

* The *official* list of current CMT Members is contained in ***Appendix A*** with their contact information.

This roster is not meant to indicate team members will work as both alternates and primary team members during an around-the-clock response. Positions will be filled with available team members as the incident warrants.

© 2017 Equifax, Inc. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000029

III. CMT General Responsibility

A. CMT Planning Responsibilities

The CMT planning responsibilities include:

- Sponsor and facilitate the development, maintenance and implementation of the CMP, assuring a high level of corporate preparedness to effectively respond to any incident that threatens the viability of Equifax.
- Participate in training and exercises to become familiar with Equifax's crisis management program.
- Review and approve policies, strategies and processes to assure crisis preparedness and effective crisis response by Equifax's corporate and business teams.
- Support the CMT Coordinator, who is responsible for coordinating CMP development, maintenance and exercising, assuring resource readiness, and coordinating CMT exercises.

B. CMT Responsibilities during a Declared Crisis

The CMT manages the overall crisis response as defined in the CMP. Specific roles and responsibilities for each CMT member are defined in **Section IV** below. The general roles of the CMT during a crisis include:

- Establish the overall strategy for managing the crisis.
- Ensure the magnitude scope and potential effects of the incident are correctly assessed.
- Ensure crisis response actions are coordinated and consistent with the incident severity.
- Consider long-term effects of the crisis by assessing potential and worst-case scenarios.
- Control and supply resources to the business unit and corporate line organization.
- Monitor and adjust People Support, IT Disaster Recovery, Business Continuity and Crisis Communication actions as necessary.
- Identify and ensure appropriate communication is maintained with key stakeholders including the Board of Directors, clients and regulators.
- Address issues and concerns of all constituencies.
- Maintain Equifax in a responsible corporate position by guiding its actions.
- Declare a crisis over, or de-escalate the status to stand-by or notify only response level.

© 2017 Equifax, Inc. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000030

C. **CMT Responsibilities after a Crisis**

Following the event the CMT may:

- As appropriate, charter an incident investigation team to determine causal factors and ensure corrective actions are taken.
- Conduct a post-incident critique to assess the effectiveness of the crisis management effort.

D. **CMT Authority**

The response intensity directed by the CMT depends on the scope of the incident and its potential or actual effect on Equifax. The CMT is authorized to mobilize all Equifax resources worldwide that it deems are required to manage a crisis and protect the health and safety of its personnel, the public and its business viability.

In addition, the CMT is authorized to acquire external resources that it deems are required to supplement its CCTs or Operational Teams, assist in protecting and restoring facilities, minimize the effects of a crisis on business operations or to fulfill any other need related to the incident.

External resources typically come from third-party providers, e.g., law firms, engineering consultants, public relations companies, third-party logistics, employee assistance providers, etc.

To the extent possible, specific contacts within each external organization should be aware of the Equifax CMP and its needs, and understand – at a minimum – the basic CMT framework and their role in supporting Equifax during a crisis. It is each CAT leader's responsibility to keep a current list of potential outside suppliers and associated contact information. In those situations where there is a high likelihood third parties would be engaged CATs should consider including key third party providers in their exercises.

© 2017 Equifax, Inc. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000031

IV. CMT Member Responsibilities

The primary responsibilities of CMT members are summarized in Table A.

TABLE A - CMT MEMBERS' RESPONSIBILITIES

CMT ROLE	Responsibilities	CAT Plan
Crisis Manager	Preparedness • Develops a thorough understanding of all plans and systems. • Reviews crisis preparedness and approves crisis management policies, plans and organizations. • May lead the CMT in exercises. • Provides guidance and direction to the CMT Coordinator. Response • Declares an incident a crisis, directs resources to activate the CMT and set up the Crisis Command Center (as defined in **Section VI).** • Assists in gathering the CMT for crisis meetings. • Manages and directs the CMT in significant incidents. • Provides primary communication to Equifax leadership. • Communicates with stakeholders of strategic interest. • Provides counsel and ultimate decision on policy changes or exceptions and position guidance. • Conducts initial meeting upon activation and schedules subsequent meetings. • Keeps the team up to date on objectives and focused on appropriate issues. • Recommends strategies and priorities and receives input to guide strategic response. • Approves communication to all stakeholders in conjunction with the Communications CMT member. • Determines the implementation timing for critical and essential business continuity activities. • Ensures all recovery issues are resourced and managed appropriately. • Declares the crisis over, or sets the CMT at the stand-by or notification only response level.	None

© 2017 Equifax, Inc. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000032

TABLE A - CMT MEMBERS' RESPONSIBILITIES		
CMT ROLE	**Responsibilities**	**CAT Plan**
Crisis Coordinator	Preparedness • Maintains Equifax Crisis Management Plan and Appendices and continuously assesses corporate preparedness. • Has audit responsibility for all other response plans (emergency response, disaster recovery, crisis communications, business continuity, etc.), i.e., works with plan owners to make sure plans are maintained and tested. • Manages crisis training/other resources for the CMT. • Schedules and oversees exercises and simulations – ensures that outcomes are addressed in related plans. • Defines the information channels for information flow for the crisis management organization. Response • Assists the CMT Leader in assessing the crisis. • Collects initial information and recommends activation level to the CMT leader. • Sets meeting particulars – including schedule, agendas, participants, use of the crisis management methodology, analytical frameworks, etc. • Looks ahead, identifies issues, considers worst-case scenarios and supports development of contingency plans to ensure continuity of response to minimize negative effects. • Provides crisis management counsel/guidance to the team. • Resources the CMT; observes overall activity versus plan. • Works closely with the CMT to coordinate production of incident briefing documentation, situation reports, action plans, etc.	None

© 2017 Equifax, Inc. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000033

TABLE A - CMT MEMBERS' RESPONSIBILITIES		
CMT ROLE	**Responsibilities**	**CAT Plan**
All CMT Members	Preparedness • Oversee policy development and interpretation, and resource CMT planning for their function. • Participates in regular planning meetings led by the CMT Coordinator and ensures adequate planning within their respective organizations. • Is familiar with the plans, procedures and teams that develop and execute crisis management actions related to specific departments and the overall Equifax. • Works with the CMT Coordinator to make changes as appropriate to maximize the ability of the crisis management organization to address the needs of the function or business they represent. • Participates in workshops and exercises to increase working knowledge and confidence in the CMT and supporting teams. • Develops a personal preparedness plan to address the needs of his or her family in a protracted crisis. • Maintains contact lists and initial guidance to engage in the process when an event occurs. • Ensures coverage is always available to staff the CMT for their function (primarily through coordination of business and personal travel schedules and work assignments). Response • Participates in the initial activation conference call to assist in determining "next steps" in the incident. • Reports to the Crisis Command Center (as defined in **Section VII**) location (physical or virtual) if requested. • Engages in the activities of the team, addressing the Equifax crisis from the strategic perspective and providing counsel and support. • Ensures departmental resources are mobilized to integrate with the CMT and supporting teams. • Ensures clear effective communication between the CMT and all members of their function or business, especially those responding. • Acts on the responsibilities defined in the following department-specific guidance on the following pages.	None

© 2017 Equifax, Inc. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000034

TABLE A - CMT MEMBERS' RESPONSIBILITIES		
CMT ROLE	**Responsibilities**	**CAT Plan**
Human Resources	• Serves as employee relations counsel to the CMT. • Ensures an accurate accounting for people, including identification of injured or missing personnel. • Arranges for liaison and assistance for affected personnel and affected family members of personnel. • Advises on counseling/EAP, or corporate employee relations support to persons involved in the crisis. • Expedites provision of medical benefits or other support relevant to an employee's health. • Oversees on-going employee communications in conjunction with Communications CMT member, including creating messages and updating all employee communication vehicles. • Has access to Equifax's payroll process and benefit plans: disability plan, health benefits, FMLA, and other benefits. • Guides/manages sensitive employee relations issues. • Decides what personnel need during a disaster in conjunction with CMT Leader. • Activates and oversees the ***People Support Plan.*** • Activates and oversees the department's ***Business Continuity Plans.***	*Appendix B*

© 2017 Equifax, Inc. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC.

TABLE A - CMT MEMBERS' RESPONSIBILITIES		
CMT ROLE	**Responsibilities**	**CAT Plan**
Information Technology	• Serves as principal Information Technology counsel to CMT. • Ensures CMT and CAT personnel have all needed technology solution available, and supports them as needed. • Manages and directs all information system resources, including information risk management, IT strategy and architecture, etc. • Manages telecommunications, computer systems, data centers and other services during a crisis. • Keep CMT and CAT members informed of IT systems and operational status. • Ensures recovery of infrastructure and application systems. Ensures the recovery is prioritized based on current business needs. • Provides support as requested by the CMT. • Make IT related decisions (ex: hardware & software purchases, domestic and /or global resources, etc.). • Coordinates information security operation activities with the Security and Safety CMT member. • Coordinates with the Communications CMT member to develop messages for customers. • Provides resources and support for the ***IT Disaster Recovery Plan.*** • Activates and oversees the department's ***Business Continuity Plans.***	*Appendix C*

© 2017 Equifax, Inc. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000036

TABLE A - CMT MEMBERS' RESPONSIBILITIES		
CMT ROLE	**Responsibilities**	**CAT Plan**
Corporate Communications	• Serves as principal communications counsel to CMT. • Responsible for all media relations, internal Equifax communications, and managing communications information related to an incident. • Establishes the media relations briefing center. • Partners with HR CMT member to assure alignment of employee communications. • Approves communications through legal counsel. • Monitors local media coverage for crisis related information and ensures correct information is being reported. • Recommends and supports the authorized corporate media spokesperson at Equifax headquarters and all other locations. • Controls the final content, timing, and method of issuing of any statements. • Coordinates activities with the Investor Relations Leader for any shareholder communications. • Coordinates activities with the IT CMT member for any customer communications. • Provides any necessary liaison with media organizations or public relations representatives of any other involved agencies or companies. • Oversees implementing and activation of the ***Crisis Communications Plan.*** • Activates and oversees the department's ***Business Continuity Plans.***	***Appendix D***

© 2017 Equifax, Inc. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000037

TABLE A - CMT MEMBERS' RESPONSIBILITIES		
CMT ROLE	**Responsibilities**	**CAT Plan**
Legal	• Serves as key advisor to the CMT for all legal advice and information, during and subsequent to an incident. • Takes all needed actions immediately to assert privilege and ensure legally responsible communications within the CMT and other response teams. • Immediately acts to preserve the official record of actions taken during the response, with the goal of reducing litigation issues. • Oversees all legal decisions and actions including civil, contractual, criminal, regulatory, labor, and investigative. • Provides legal advice and counsel to ensure full and timely disclosure is made to regulatory and/or legislative authorities. • Provides legal advice and counsel for all response activities to reduce liabilities. • Activates and oversees the department's ***Business Continuity Plans.***	***Appendix E***

© 2017 Equifax, Inc. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000038

TABLE A - CMT MEMBERS' RESPONSIBILITIES		
CMT ROLE	**Responsibilities**	**CAT Plan**
Finance	• Serves as principal financial adviser to the CMT. • Coordinates with the Communications CMT member and the Investor Relations Leader to provide message content for employees, customers, vendors, shareholders and the financial community. • Establishes financial impact of the crisis. • Estimates cash flow projections and evaluates potential needs to draw on credit revolver. • Tracks all financial impacts. • Ensures internal controls are in place. • Sets financial policy and approves financial strategies. • Works with Legal CMT member to assure full and timely disclosure to financial regulatory agencies. • Verifies financial operations (Cash Collections, AR, AP, Payroll) continue as practical. • Directs insurance activities and coordinates with insurance carriers and claims adjustors. • Advises CMT on insurance policy coverage, deductibles and caps to help guide response to the crisis. • Provides finance-related advice, information, and support during and subsequent to a crisis. This includes: o Arrangements for timely, discreet cash availability. o Advising teams regarding concerns about surrounding tax liabilities for corporate and/or subsidiary locations involved in an incident. o Determining the procedures to be used in accounting for funds needed, while at the same time protecting information regarding their intended use. o In the event of extortion or a kidnapping event, the CMT Team Leader will activate the ***Serious Crime Plan*** and make the appropriate notifications. • Serves as primary CMT contact for insurance claims management. • Activates and oversees the department's ***Business Continuity Plans.***	*Appendix F*

© 2017 Equifax, Inc. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000039

TABLE A - CMT MEMBERS' RESPONSIBILITIES		
CMT ROLE	**Responsibilities**	**CAT Plan**
Global Operations	• Serves as principle business operations advisor to the CMT. • Ensures all operations personnel are accounted for and informs CMT members of functioning staffing level. • Takes all necessary steps to ensure service requests are being processed, and advises CMT members of any critical interruptions to operational processes. • Continuously monitors all transactions to prevent fraud, especially under abnormal operating situations • Monitors disruptions to service level agreements, identifies financial operating risk associated in conjunction with the CMT, and recommends strategies to minimize risk and restore effective service levels. • In partnership with Sales, coordinates activities with Corporate Communications on any customer, partner, and/or vendor communications. • Monitors the effects of the incident on the ability to manage back office operations, and takes actions to minimize disruption and financial operating risks associated with disruptions. • Monitors the effects of all other critical transaction-based operations, advises the CMT about these effects and recommends strategies to minimize disruptions and reduce financial operating risk. • Verifies that the client service operations are operational or manages plans to return those operations to service as soon as possible and appropriate. • Ensures all client service operation have the correct messages for clients related to the crisis, crafted by and in conjunction with the CMT Communications member. • Activates and oversees the department's ***Business Continuity Plans.***	***Appendix G***

© 2017 Equifax, Inc. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000040

TABLE A - CMT MEMBERS' RESPONSIBILITIES		
CMT ROLE	**Responsibilities**	**CAT Plan**
Security	• Serves as principal Security & Life Safety advisor to the CMT. • Manages and directs Security & Life Safety resources. • Approves the safety and security of any location where the CMT and CATs may assemble PRIOR to assembling the teams. • Assures the assembly locations remain safe and secure for the duration of the response. • Assess threats to executive members' personal residences and takes needed action to protect them. • Insures all needed Information Security actions are taken to protect confidential data and to prevent unauthorized access or use of Equifax system or data. • Acts as a resource to local responders regarding all Security & Safety aspects, including deployment of site Emergency Response plans. • Oversees implementing and activation of the ***Equifax Security Incident Response Plan.*** • Oversees reporting of physical, medical, and cyber related incidents to governmental authorities, in conjunction with affected sites. • Works with CMT to comply with regulatory investigations and recommendations. • Serves as primary CMT law enforcement liaison. • Manages and directs security resources for corporate offices. • Manages executive security and site security globally. • Assures safety of executives in route to and at incident scene. • Provides functional expertise, as needed, in a kidnapping or hostage situation. • Arranges for 24/7 personal security for any executives. Providing liaison and coordination with appropriate law enforcement agencies and specialized security consultants, as directed by the CMT. • Ensures all official documents are properly controlled and handled as potential evidence (as directed by Legal), which may be required to assist in investigations. • Advises CMT about access control practices for Equifax property for affected locations. • Coordinates information security activities with the Information Technology CMT member. • Oversees the affected site's ***Emergency Response Plan.*** • Activates and oversees the department's ***Business Continuity Plans.*** • Directs the **Security Incident Response Team**	***Appendix H***

© 2017 Equifax, Inc. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000041

TABLE A - CMT MEMBERS' RESPONSIBILITIES

CMT ROLE	Responsibilities	CAT Plan
Real Estate	Facilities Aspects I. Serves as principal facilities liaison to the CMT. • Manages facility services to support the CMT, including set-up of the various command centers and other CAT meeting locations. • Secures accommodations, travel and food for response teams. • Directs site response through site management. • Assists in relocation planning if needed. • Manages disruptions in mailroom operations, ensuring documents are protected and third-party vendors are informed about any delivery/pick up disruptions. • Oversees the ***Crisis Command Center Plan,*** including setting up and supporting all facilities used for the CMT, supporting teams, and other staff involved in responding to the crisis. Travel Aspects • Requests travel records as needed • Acts as primary CMT travel advisor • Ensures Travel Department coordinates with the HR CAT to: o Help account for people by identifying personnel on travel o Identify the location of travelers when a disaster strikes that effects the ability to travel o Provide assistance to travelers affected by a disaster • Manages expedited travel arrangement for the CMT, CAT members or the On-scene team as required. Procurement Aspects • Assesses the effects of the incident on inbound and outbound shipments. • Manages contacts with suppliers to alter purchase or delivery locations to accommodate for the incident. • Ensures that key procurement personnel are readily available to support the CMT's responses, regardless of location. This includes maintaining up-to-date telephone contact lists of vendors and ensuring personnel have access to a safe working environment, communication facilities, computer equipment and data necessary for real time, uninterrupted actions in support of continuing operations. • Works with finance and treasury to ensure that contractual obligations continue to be met. • Assesses the financial impact of contractual obligations on Equifax as a result of the crisis. • Works with legal and other CMT members to determine if force majeure other declarations must be made under contracts • Activates and oversees the department's ***Business Continuity Plans.***	*Appendix I*

© 2017 Equifax, Inc. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000042

TABLE A - CMT MEMBERS' RESPONSIBILITIES		
CMT ROLE	**Responsibilities**	**CAT Plan**
Marketing, Analytics & Data Services	• Serves as primary marketing, analytics and data services advisor to the CMT. • Provides strategic guidance and tactical execution on all aspects associated with the four "Ps" of marketing, including marketing communications, product development and management, pricing, market and customer insights, strategy and channel management. • Provides strategic guidance and tactical execution on all aspects associated with analytics and data services, including development and management of scores and models, acquisition and loading of data, and data quality management. • Monitors the effects of the incident in product and model performance and data acquisition and loading processes. • Ensures an accurate accounting of marketing, analytics and data services personnel. • Manages risk assessment and makes policy decisions specific to the situation. • Activates and oversees the department's ***Business Continuity Plans.***	***Appendix J***

Note – Corporate Communications is captured in separate section.

© 2017 Equifax, Inc. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000043

TABLE A - CMT MEMBERS' RESPONSIBILITIES		
CMT ROLE	**Responsibilities**	**CAT Plan**
Global Consumer Solutions	• Serves as primary Global Consumer Solutions advisor to the CMT. • Provides strategic guidance on all aspects associated with the delivery of credit scores and/or credit monitoring services through the Equifax web site. • Manages risk assessment and makes policy decisions specific to the situation. • Mitigate and/or avoid any service interruptions for Equifax customers, clients or partners. • Coordinates activities with Corporate Communications disseminating information to customers, suppliers and partners. • Activates and oversees the department's ***Business Continuity Plans.***	***Appendix L***

© 2017 Equifax, Inc. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000044

TABLE A - CMT MEMBERS' RESPONSIBILITIES		
CMT ROLE	**Responsibilities**	**CAT Plan**
Workforce Solutions	• Serves as primary Workforce Solutions advisor to the CMT. • Provides strategic guidance on all aspects associated with the delivery of employment and income verifications services, unemployment claim services, compliance services, and the employment database. • Manages risk assessment and makes policy decisions specific to the situation. • Mitigate and/or avoid any service interruptions for Equifax customers, clients or partners. • Coordinates activities with Corporate Communications disseminating information to customers, suppliers, partners and governmental bodies. • Activates and oversees the department's ***Business Continuity Plans.*** • Directs the **Mid-West Regional Crisis Action Team**	***Appendix M***

© 2017 Equifax, Inc. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000045

TABLE A - CMT MEMBERS' RESPONSIBILITIES		
CMT ROLE	**Responsibilities**	**CAT Plan**
International	• Serves as primary international Business Unit advisor to the CMT. • Provides strategic guidance on all aspects associated with the international delivery of credit and other data services. • Manages risk assessment and makes policy decisions specific to the situation. • Mitigate and/or avoid any service interruptions for Equifax customers, clients or partners. • Coordinates activities with Corporate Communications disseminating information to customers, suppliers and partners. • Maintains a liaison with each regional leader regarding any country specific incident and/or crisis. • Activates and oversees the department's ***Business Continuity Plans.***	***Appendix N***

© 2017 Equifax, Inc. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000046

TABLE A - CMT MEMBERS' RESPONSIBILITIES		
CMT ROLE	**Responsibilities**	**CAT Plan**
Corporate Development	• Serves as primary emerging markets advisor to the CMT. • Serves as primary corporate development, emerging markets and M&A advisor to the CMT • Provides strategic guidance on all aspects associated with the development and delivery of credit and other data service products in emerging international markets. • Manages risk assessment and makes policy decisions specific to the situation. • Mitigate and/or avoid any service interruptions for Equifax customers, clients or partners. • Coordinates activities with Corporate Communications disseminating information to customers, suppliers and partners. • Activates and oversees the department's ***Business Continuity Plans.***	***Appendix O***

© 2017 Equifax, Inc. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000047

TABLE A - CMT MEMBERS' RESPONSIBILITIES		
CMT ROLE	**Responsibilities**	**CAT Plan**
USIS	• Serves as primary consumer information solutions advisor to the CMT. • Provides strategic guidance on all aspects associated with the delivery of decision making products and services. • Manages risk assessment and makes policy decisions specific to the situation. • Mitigate and/or avoid any service interruptions for Equifax customers, clients or partners. • Coordinates activities with Corporate Communications disseminating information to customers, suppliers and partners. • Activates and oversees the department's ***Business Continuity Plans.*** Directs the **US Information Solutions CAT.**	***Appendix Q***

© 2017 Equifax, Inc. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000048

TABLE A - CMT MEMBERS' RESPONSIBILITIES		
CMT ROLE	**Responsibilities**	**CAT Plan**
Regional Leadership (Local international response)	• Acts as primary counsel to the CMT on all aspects of the operation in his or her area of responsibility including: o Local governmental requirements and laws. o Cultural expectations and norms. o Local conditions such as community reactions, media coverage, physical conditions, etc. o Travel logistics. o Security conditions. • Provides on-site presence to assist in managing the event, as directed by the CMT. • Acts as Equifax spokesperson, as directed by the CMT. • Oversees the entire local response for regions under his or her control. • Activates and oversees the region's ***Business Continuity Plans.*** • Oversees the appropriate **Regional CAT**. **NOTE**: The regional leadership has both regional sales responsibility, and some amount of an operational role, including HR, IT, Communications, Finance, Security, etc. For each of these roles, the appropriate responsibilities are the same as listed in the various sections above. In essence, the regional leadership, during a crisis, needs to manage all aspects of the local response, and therefore should have a detailed plan to do this through their Regional CAT.	***Appendix R***

© 2017 Equifax, Inc. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000049

V. Site Emergency Response Team Leader/Command and Communications Unification

A. Equifax Emergency Response

The number of trained emergency response staff at each Equifax locations varies by location depending of the number of personnel at the location and other factors. All sites have established Emergency Action Plans. Locations with sole occupancy have an established ***Emergency Response Team*** and trained emergency responders. Locations without sole occupancy have assigned personnel, typically an office manager or most senior leader in the office, to be responsible for emergencies. At these smaller locations emergency response procedures are defined in the Equifax ***Life Safety Guidelines***.

A list of locations with the level of emergency response capabilities is maintained by the CMT member responsible for Security & Safety. During a site emergency, the emergency response aspects of the incident will be managed according to the type of plan in place.

If a crisis is declared in response to a site emergency, the site emergency response representative will:

- Implement the emergency response plan or general emergency guidelines for the site.
- Manage and direct all Equifax emergency response resources at the incident scene or related to the incident scene, including the CMT on-scene team.
- Designate an on-scene person to communicate with the CMT.
- Designate the on-scene Equifax spokesperson as appropriate (spokespersons to be approved in advance by Communications).
- Determine if external emergency responders should be called.

B. CMT On-scene Team

The On-scene Team is dispatched to an incident by the CMT. They provide support to the Site Incident Commander, assess additional company needs for crisis response, and keep the CMT informed of events at the scene. The On-Scene Team Leader or Communications Member may act as a local company spokesperson in lieu of site management. Any CAT member may be designated to participate as an On-Scene Team member. The On-Scene Team may also include site personnel dedicated to corporate response activities at the time of the incident.

The On-scene Team makeup will vary with the type of crisis but usually includes representatives from the affected business, Operations, Communications, HR, and Legal. Typical members and primary responsibilities are listed in Table B.

© 2017 Equifax, Inc. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000050

Table B
CMT On-Scene Members Responsibilities*

On-Scene Member	Responsibilities	Member Selection
Affected Department/ Operations	• Team Leader for the On-Scene Team • Provides guidance to Site Incident Commander, and site line management • Assesses effects of incident and keeps affected Department management and CMT informed	Representative(s) is designated by affected Department Leader based on responsibility, authority, and knowledge of site, product, process, or operation involved
Legal	• Evaluates extent and nature of incident • Coordinates legal support personnel on scene • Supervises implementation of legal strategies and tactics on scene • Directly manages claims process • Accompanies regulatory agencies on incident investigations • Keeps CMT informed	Senior level attorney as designated by GC General Counsel
Communications	• Provides on scene crisis communication advice • Assesses local employee and public reaction, recommends strategies and tactics for improved communication, and provides site public relations and media support • Serves as the primary liaison between site spokesperson and Public Information Officer • Attends and assesses all local press briefings • Keeps Communications CAT informed of crisis incident status	Communications CAT member or Outside Resource
Human Resources	• Provide assistance in coordinating HR response • Assess need for counseling for impacted employees and community members • Evaluates on scene security requirements needed for protecting facility and personnel • Coordinates and assists in providing security resources and controls and keeps CCMT Security member informed on security issues	Human Resources CAT members
Other Functions	• Provides support in all aspects of on scene incident response and communications as directed by CCMT	Determined when crisis occurs by CCMT

© 2017 Equifax, Inc. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC.

C. **External Emergency Response Command Unification**

If the emergency requires an external response, e.g., if 9-1-1 (or similar external emergency dispatchers in international locations) is called or a fire alarm is activated, then leadership of the emergency response is taken over by local (non-Equifax) emergency responders. In this case, the local officials will usually establish an Emergency Operations Center ("EOC") and designate a local Incident Commander. The local Incident Commander is typically the Fire Chief or Police Chief. In extreme situations, state or federal emergency responders may take over the local Incident Commander's role.

If an external response is active, the site emergency response representative will also:

- Unify command with the local Incident Commander, by using the Incident Command System* protocol followed by most federal, state and municipal agencies.
- Coordinate resources and response tactics with the local Incident Commander

* Most city, county and state response organizations in the US, use the Incident Command System ("ICS"), a standardized on-scene emergency management system, which includes an integrated organizational structure designed to reflect the complexity and demands of single or multiple incidents without being hindered by jurisdictional boundaries. (International locations may or may not have a similar system.) The ICS model uses a combination of facilities, equipment, personnel, procedures, and communications protocols operating within a common organizational structure. It is intended to aid in managing resources during emergencies and is applicable to both small and large incidents. The ICS plan provides a process for private sector representatives to assume various positions in the on-scene incident command post and the Emergency Operations / Joint Information Center for the lead responding agency.

D. **External Communications Unification**

External Communications: The external (community and media) communications aspects of most emergencies are coordinated by a local (non-Equifax) Public Information Officer ("PIO") who usually accompanies and reports to the local Incident Commander. The Equifax communications lead at the site will work closely with the PIO to manage media and community communications activities.

© 2017 Equifax, Inc. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000052

VI. Operational Guidance

A. Incident Resolution or Escalation

Most incidents will be resolved without activation of the CMT.

One Shift Response: CMT activation and staffing is at the discretion of the CMT Leader or designate. In most responses, the primary and alternate CMT members will activate together and will manage the incident to a satisfactory conclusion. In this case, the CATs may be led by either the assigned CMT leader or by the CMT alternate as determined by the CMT members and availability. If both members for a specific role activate, one of the members can report to the CAT team once a one-shift response is declared.

Two Shift Responses: If the incident could require an extended continuous response, the CMT should identify two teams to work in shifts. In addition, two teams may be required for each CAT. **Managing team schedules and hourly operating guidance is the responsibility of the CMT Coordinator.**

The specific number and level of CMT members and CAT teams activated will be determined by the CMT Leader. **However, whenever any type of activation occurs, all primary and alternate CMT members will be, at a minimum, alerted about the incident.**

B. Incident Notification, Threat Assessment and CMT Activation

It is critical that all locations quickly report any and all potential crisis situations to their department management or security. This must be done as soon as possible, regardless of the time of day or night, preferably within 30 minutes of the incident.

If a senior department leader cannot be reached immediately, any employee with information about a potential crisis should call the Equifax Security Hotline to report the incident.

Notification of incidents that are, or have the potential to become, an Equifax crisis should be directed to the Equifax 24-hour Security Hotline by calling:

+1 770.740.5555

The Security Hotline Line is available 24/7/365 to receive and forward crisis information to CMT representatives on the Incident Assessment Team. The specifics for handling any incident reported to the Security Hotline are found in ***Appendix A - Incident Notification and CMT Activation Procedures***.

© 2017 Equifax, Inc. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000053

C. Incident Assessment Coordinator - Activation Decisions

Appendix A contains the procedure used by the Security Hotline staff if an incident is reported. In general, they will activate the Incident Assessment Team using the Mass Notification System.

The Incident Assessment Team will assess the threat, seek guidance from other leadership if needed (e.g., IT Operations, Facilities, Client Advisory Services, etc.), and then determine the level of CMT activation required. The Incident Assessment Team includes:

1. Mike Douglas
2. Dodd Williams
3. Susan Mauldin

Before activating the CMT, the Incident Assessment Coordinator will decide on an appropriate initial activation level based on the specific circumstances of the incident. The activation level can escalate as necessary to acquire appropriate corporate resources for crisis response. (See **Section D** for activation levels.) All serious incidents must be reported to the CMT Leader or designate immediately. If there is any doubt about the correct activation level, the CMT should be, at a minimum, activated at the **Notify Only Level** as described in **Section D.1**.

D. Plan Activation Levels

There are three CMT activation levels. The **Notify Only Level**, **Stand –By Level** and **Respond Level** are used to establish awareness of a potential crisis or to activate the CMT in response to an actual crisis. Each level is described below:

1. Notify Only Level

The CMT is notified when an incident is not an obvious Equifax crisis initially, but which warrants monitoring or would be of interest to members of the CMT. At this level, **CMT Members DO NOT respond or assemble**. Members are typically informed of the event during normal hours, typically via e-mail, and the CMT Coordinator becomes responsible for tracking incident status. Examples include:

- A minor fire or explosion at a facility where on-site resources are deemed sufficient to handle the event and there are no serious injuries, or
- Any event that has a reasonable potential to escalate in scope and thereby harm Equifax's reputation, assets or personnel, including an event in a neighboring facility.

2. Stand-by Level

The CMT may be put on "Stand-by" when an incident has the potential to become a Equifax crisis but CMT assembly is not yet appropriate. During this stage, CMT members will be notified of the incident and placed on notice that the team may be activated in the future. CMT members should then be making the appropriate arrangements to ensure the CAT is staffed for their function. **CMT Members DO NOT assemble at the Stand-by level.**

© 2017 Equifax, Inc. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000054

3. **Respond Level**

The CMT will be activated when there is a high potential for a Equifax crisis to occur. The activation can occur immediately upon initial notification or as an event escalates from a lower activation level. All CMT members will be notified of the incident and be asked to attend an initial briefing. Declaring a "Respond-level" activation immediately invokes the Equifax Crisis Management Plan and initiates an initial CMT briefing.

4. **Partial Activation**

The CMT is staffed by both executive-level and VP/Director-level staff. In minor to severe incidents, or in situations that clearly do not warrant a full team response, the CMT may assemble as a partial team, based on the direction of the CMT leader or designee.

E. **De-escalation from Respond Level Activation**

The CMT, once activated, is a self-managed team. The level of activity, frequency of meetings and number of active members should match the current needs to effectively manage the incident, and maintain command and control over responders. At some point, most incidents will become business recovery focused, versus crisis management focused. When appropriate, typically upon consensus of the CMT, the CMT Leader can declare the crisis to be over and disband the CMT. If the CMT is de-escalated to the Notify Only Level, the CMT should follow the guidance above until it is fully deactivated.

F. **CMT Action Lists**

CMT Action Lists contained in **Part II: CMT Response Plan**, are used to implement basic crisis response activities. Although each crisis is unique, the lists provide a framework for typical crisis response activities, and are provided to each CMT member as they arrive at the Crisis Command Center.

G. **Communication with the Board of Directors**

If the Board of Directors needs to be engaged or informed of the incident, the responsibility of their notification is owned by the following person(s):

- Rick Smith (Primary)
- John Gamble (Secondary)
- J. Kelley (Alternate)

© 2017 Equifax, Inc. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000055

VII. Facilities and Equipment

A. Equifax's Security Hotline - +1 770.740.5555

The Security Hotline is available 24/365 to receive calls reporting all incidents related to Equifax operations, systems or products. See ***Appendix A*** for detail on how the Crisis Line operates. Please NOTE this number is a Voice Over IP ("VOIP") number and may not operate correctly in certain situations.

B. Equifax's Crisis Management Bridge Line

In most situations, the initial CMT assembly procedure will be to meet on a bridge line. This accomplished two things: 1.) It allows for faster response during non-working hours, and 2.) It allows Security resources to assess the security and safety of any physical meeting locations before assembling the CMT. The CMT Bridge Line is:

Dial in: Redacted
Access Code: Redacted Leader Code: Redacted

C. Equifax Crisis Command Center

Equifax's Crisis Command Center (CCC) is the facility that will house and support the CMT and the CATs. It is also the central point for incoming and outgoing communications with key constituencies. The facility can handle a high volume of calls resulting from inquiries to Equifax during a crisis.

The ***primary*** CCC is located at 1550 Peachtree Street if a full CMT/CAT activation is required. Meeting rooms have been established for the CMT and for each CAT, along with a place to brief the media. Equipment and other resources required to effectively respond to an incident will be provided by the Facilities and IT organizations as part of their CAT plan. The CMT will typically meet in the Centennial Conference Room on the 6th Floor of 1550 Peachtree Street.

The ***alternate CCC*** is at the Mount Vernon Conference Room on the 3rd Floor of 500 Northpark office. See ***Appendix F – Office Facilities Crisis Action Team Plan.***

An additional **backup CCC** can be the Executive Briefing Center on the 1st floor of Building 1 of the JV White campus.

Additional facilities can serve as an alternate CCC, and are identified and acquired under the direction of the CMT Leader and Facilities CAT at the time of an incident.

D. Crisis Communications Center

As conditions warrant, a Crisis Communication Center may be established. This facility is ideally located in a separate area away from any of the CMT or CAT rooms. This location may be used to monitor the media and develop media messaging. A full description of the facility is in ***Appendix B - Communication Crisis Action Team Plan***.

E. Media Briefing Center

The Communications CAT will take the lead on media briefings, working with the public sector incident command as necessary. A media briefing center can be established quickly with the help of the Facilities CAT.

© 2017 Equifax, Inc. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000056

F. Other Equipment

Equifax maintains additional equipment and other resources to use in a crisis, including telecommunications equipment, computer equipment, maps, building drawings, copies of plans, client contact lists, etc. Specific details about these facilities and equipment are in ***Appendix F –Facilities Crisis Action Team Plan.***

VIII. Maintenance and Training

The CMT will review the CMP on an annual basis and revise as needed. The Crisis Coordinator will facilitate this review. Each CMT member has 3 copies of this plan: one for the office, one for the car and one for the home. When the plans are revised, the Crisis Coordinator is responsible for retrieving obsolete plans and distributing new plans.

CMT and CAT will be maintained through a combination of training and exercises. The frequency of these activities will be as follows:

- Walk-thru/Tabletop exercise - CMT .....Annually to every 2 years

Training of new CMT members will be conducted on an as needed basis.

© 2017 Equifax, Inc. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000057

IX. Revision History

Date	Name	Version	Description of Changes
2/2013	Mike Douglas	1.0	Initial version of document
5/2013	Mike Douglas	1.1	Edit members
9/2013	Mike Douglas	1.2	Member revision
11/2013	Mike Douglas	1.3	Member revisions
10/2014	Mike Douglas	2.0	Annual Review/Update
4/2015	Mike Douglas	3.0	Annual Review/Update
9/2015	Mike Douglas	3.1	Member revisions
6/2016	Mike Douglas	4.0	Annual review/revisions
5/2017	Mike Douglas	5.0	Annual review/revisions

© 2017 Equifax, Inc. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000058

X. CMT Support Plans

Equifax CMP Part II – Crisis Management Team Response Plan

App A - EFX Notification and Activation Plan

Regional Crisis Action Team Plans (CATs):

Argentina Crisis Action Team

Canada Crisis Action Team

Central America Crisis Action Team

Chile Crisis Action Team

Ecuador/Peru Regional CAT Plan

Iberia Crisis Action Team

India Crisis Action Team

Midwest Regional CAT Plan

Northeast Regional CAT Plan

Paraguay Regional CAT Plan

Russia Crisis Action Team

Southeast Regional CAT Plan

Southwest Regional CAT Plan

UK Regional Crisis Action Team

Uruguay Crisis Action Team

West Coast Regional CAT Plan

© 2017 Equifax, Inc. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000059

EQUIFAX, INC., "CORPORATE CRISIS MANAGEMENT PLAN, PART II"

EQUIFAX

Corporate Crisis Management Plan

Part II: Crisis Management Team Response Plan

June 2016

Version 4.0

This document contains guidance for each Crisis Management Team member to use during a declared crisis.

Primary CMT Assembly Point	Centennial Conference Room 6th Floor of 1550 Peachtree Street.
Secondary CMT Assembly Point	Lanier Conference Room 1st Floor of JV White Building 2
Conference Bridge Line	Redacted Access Code: Leader Code: Redacted

Corporate Crisis Management Plan Part II

Crisis Management Team Response Plan

Table of Contents

© 2016 Equifax, Inc. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000061

THIS SECTION OF THE PLAN IS USED DURING A CRISIS

The CMT Action Lists, beginning on page 4, are used during crisis response. They list and briefly describe basic crisis management activities. These activities have been reviewed and approved by the CMT and are to be considered and implemented, if appropriate, in response to an incident declared to be a corporate crisis. Pages 2 and 3 describe the overall response process.

I. Basic Response Framework Overview

Phase 1: Assess the Situation & Assemble the Team

A. Event reported to Incident Manager for activation assessment.

The Incident Manager assess the threat, seek guidance from other leadership if needed (CEO, BU Heads), and then determine the level of CMT activation required. The Incident Manager is notified via the Security Desk and/or a member of the Equifax Management Team and includes:

Mike Douglas Dodd Williams Susan Mauldin

Before activating the CMT, the Incident Manager will decide on an appropriate activation level based on the specific circumstances of the incident. The level can escalate as necessary to acquire resources for crisis response. All serious incidents must be reported to the CMT Leader or designee immediately. If there is any doubt about the activation level, the CMT should be, at a minimum, activated at the **Notify Only Level**.

B. Activation Level Decision: No Action, Notify Only, Stand-by, Respond.

1. **Notify Only Level**
   The CMT is notified when an incident is not an obvious Equifax crisis initially, but which warrants monitoring or would be of interest to members of the CMT. At this level, **CMT Members DO NOT respond or assemble**. Members are typically informed of the event during normal hours, typically via e-mail, and the CMT Coordinator becomes responsible for tracking incident status.

2. **Stand-by Level**
   The CMT may be put on "Stand-by" when an incident has the potential to become a Equifax crisis but CMT assembly is not yet appropriate. During this stage, CMT members will be notified of the incident and placed on notice that the team may be activated in the future. CMT members should then be making the appropriate arrangements to ensure the CAT is staffed for their function. **CMT Members DO NOT assemble at the Stand-by level.**

3. **Respond Level**
   The CMT will be activated when there is a high potential for a Equifax crisis to occur. The activation can occur immediately upon initial notification or as an event escalates from a lower activation level. All CMT members will be notified of the incident and be asked to attend an initial briefing. Declaring a "Respond-level" activation immediately invokes the Equifax Crisis Management Plan. CMT activation will typically use the Mass Notification System.

© 2016 Equifax, Inc. All Rights Reserved

C. Communicate to CMT if needed.

In all situations when the Incident Manager has determined the incident warrants CMT activation at any level, CMT members will be notified as described above. If the CMT is assembled, the Mass Notification System will be activated and simultaneous communication to all CMT members and alternate members will occur. All documented contact points will be involved (Office Phone, Cell Phone, Home Phone, E-mail, etc.). In most cases, a conference line will be provided as part of the activation process.

D. Only proceed to Phase 2 if a RESPOND level activation is declared.

Phase 2: Prepare to conduct the Initial Briefing

- Collect information.
- Prepare agenda (next page).

Phase 3: Conduct the Initial Briefing (For all CMT members and alternates–usually a call)

- Brief team.
- Discuss actions that are required immediately.
- Specify next meeting time/location.
- Discuss CAT activation.
- Activate CATs and review situation. Get CAT input.

Phase 4 Conduct second meeting (CMT assembles)

- Use pre-determined agenda (next page).
- Status report from affected site/business.
- Status reports from each function (include information from CAT briefings).

Phase 5 Continue Response Activities

- Conduct routine meetings using Brief, Discuss, Action model.
- Continue management of crisis.

Phase 6 Conclude the crisis response (Recovery)

- Stand down CMT – move into recovery stage.
- Assign responsibility for on-going management efforts.
- Charter incident investigation team as necessary.
- Conduct After Action Review.

© 2016 Equifax, Inc. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000063

II. Initial Actions - CMT Leader/Coordinator Guidance

Review Guiding Principles and Priorities:

1. Place the highest priority on Life Safety – the welfare of all people including personnel, clients, visitors, emergency responders and community members.
2. Protect our assets and preserve our ability to operate and supply our clients.
3. Maintain a strong Equifax reputation through ethically and socially aware behaviors that ultimately preserve shareholder value.

AFTER Declaring a Crisis

Initial Notification (Note: ***Appendix A*** describes CMT activation process in detail.)

- Receive briefing from Incident Assessment Coordinator.
- Confirm decision to activate CMT.
- Confirm plan for initial CMT briefing.
  - Time, location, call-in numbers, etc.
- Consider the need to inform the Equifax Corporation or Board of Directors.
- Consider the need to inform Equifax's regulatory agencies (OSHA, EPA, DOT, etc.)

Prepare for initial CMT briefing

- Review the Initial CMT Briefing Agenda (below) to confirm responsibilities.
- If possible, obtain an updated status of the incident.
- Consider the timing for the first full CMT meeting.

Agenda Topic	Desired Outcomes
Purpose of the call	Brief the Team. Direct Admin Support member to document all facts and decisions.
Identify all callers	Document all callers and ensure all CMT roles are represented.
Situation Description	Provide the current details of the situation to the CMT.
Support	Identify support requested by the site or business. Discuss the potential additional support the CMT may be required to provide.
Team Selection	Identify the team members (name and role) that will continue to support this event.
Communications	Determine what communications have been made and what communications are still required. Assign responsibilities.
Logistics	Announce next meeting time and location (meeting room and telephone numbers).
Adjourn meeting	Final concerns issues. Direct CMT members to assemble, brief and provide direction to his or her CAT.

© 2016 Equifax, Inc. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000064

Conduct the Initial Briefing

- Call-in early and lead Initial Briefing.
  - Standard call-in information:

Virtual Command Center
Bridge #: Redacted
Passcode: Redacted

International: Redacted
Passcode: Redacted

Leader code: Redacted

- Follow the Initial CMT Briefing Agenda.
- Remind participants of the guiding principles and priorities
- The Administrative Support member will capture names of CMT members that will continue to participate in the response.
- The time and location of the next CMT meeting will be announced.
  - Pre-designated room is the Centennial Conference Room on 6th Floor at 1550 Peachtree.
  - Any other facility can be designated as the meeting location if needed. Choices include:
    1. Mount Vernon Conference Room, 500 Northpark.
    2. Executive Briefing Center, Building 1, JV White Campus
    3. Any other locations determined by CMT leader

Note: It is important for the CMT Leader to project a calm, confident and positive attitude to the team. Acknowledge that not everything will be perfectly executed as designed. Decisions will need to be made with incomplete information. Encourage people to ask questions if they are uncertain of information or decisions. Reinforce this is a team effort.

© 2016 Equifax, Inc. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000065

CMT Leader Guideline for First/Ongoing CMT Meeting

- Ensure phone lines are open.
- Roll Call – Identify participants/ ensure all roles are represented.
- Establish / enforce the Briefing/Discussion/Action CMT meeting process. (See next page.)

Briefing Phase

1. Provide Event Status Update.
2. Departmental Status Updates (CMT Leader/Each CMT Member).

Discussion Phase

1. Review key decision making priorities with the team.
   a) Place the highest priority on Life Safety – the welfare of all people including personnel, clients, visitors, emergency responders and community members.
   b) Protect our assets and preserve our ability to operate and supply our clients.
   c) Maintain a strong Equifax reputation through ethically and socially aware behaviors that ultimately preserve shareholder value.
2. Reminder of Key Roles.
   - The affected site/business has the primary responsibility for managing a physical event. The CMT's role is to support the site/business, not to assume direct management of the local response.
3. Identify key objectives for the CMT to accomplish.
4. Communications.
   - Agree on process and timing for communicating to key stakeholders.
   - Agree on content of messages (or holding statements).
   - Assign and confirm responsibility for communicating to Board of Directors.
   - Assign and confirm responsibility for communicating to regulatory agencies.
5. If appropriate, assign a CMT member to lead a Stakeholder Analysis.
   - Resources Evaluation – Does the CMT need any additional resources?

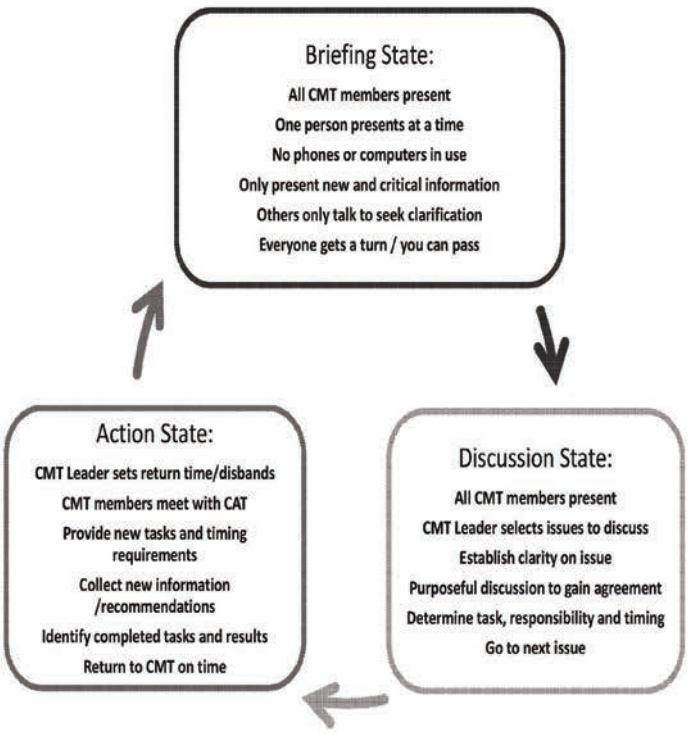
Action Phase

1. Announce time for next CMT meeting and disband group (CMT Leader).
2. Review status of response so far, and determine agenda for next meeting.

© 2016 Equifax, Inc. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000066

CMT Meeting Process



© 2016 Equifax, Inc. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000067

III. Crisis Management Team - Actions Lists

Note: These action lists are not all-inclusive. Not all actions should be implemented in every situation. The action lists do not replace use of good judgment. Every situation will require additional actions based on the strategic and tactical requirements of the event.

A. Crisis Leader/Coordinator

- ❑ Enforce the Briefing/Discussion/Action CMT meeting process.
- ❑ Prepare for and conducting meetings.
- ❑ Request CMT members to assemble CATs and assign tasks if appropriate.
- ❑ Ensure Administrative Support records the facts of the incident so all can see them. This documentation will also become the official record of the response. Consider the need for legal personnel to assist in this process.
- ❑ Coordinate an initial briefing with CMT members on the current situation.
- ❑ Coordinate situation report from the site emergency response team, Safety and Security, IT, or business leadership, based on which person has the best information. Ensure Communications flow.
- ❑ Participate in the preparation of an action plan.
- ❑ Consider need to contact and assemble Board of Directors.
- ❑ For extended responses, establish work-rest schedule for the CMT.
- ❑ For long-term responses, oversee planning and execution for shift changes for CMT and CATs.
- ❑ Ensure planning and communications meetings are conducted as necessary.
- ❑ Move into the managed crisis mode, continuing to perform any above CMT Leader tasks on an ongoing basis until the crisis is stabilized. Continue to diagnose the effects of incident; including data loss and continuity risk.
- ❑ Decide when to begin "Return to Normal" planning, making sure to consider operational status, emotional condition of Equifax employees, regulatory status, and perceptions of media and society.
- ❑ Begin to create "Return to Normal" or demobilization Plan to return the business to the restored or new location.
- ❑ Notify the CAT leaders to instruct their teams on what to do in "Return to Normal" situation.
- ❑ Conduct the post incident review.

© 2016 Equifax, Inc. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000068

Note: These action lists are not all-inclusive. Not all actions should be implemented in every situation. The action lists do not replace use of good judgment. Every situation will require additional actions based on the strategic and tactical requirements of the event.

B. Human Resources

People Support Aspects

- ❑ Review with CMT leader the appropriate HR response level.
- ❑ Provides strategic HR and employee/labor relations leadership to the CMT.
- ❑ Communicate the accounting-for-people process to CMT members.
- ❑ Coordinate with Communications CMT member on all messaging and distribution of information about the incident to personnel Equifax-wide.
- ❑ Recommend to CMT leader if an all-employee meeting is required.
- ❑ Assemble Human Resources CAT, brief them, solicit recommendations and concerns, assign tasks to them and establish a periodic review cycle to maintain collaboration between the CMT and Human Resources.
- ❑ Oversee implementation of the Equifax ***People Support Plan.***
- ❑ Oversee implementation of the department's ***Business Continuity Plan.***
- ❑ Oversee HR CAT responsibilities:
  - o Account for ALL personnel, visitors, and other people that were at the site when the incident occurred. (See ***HR CAT Plan*** and ***People Support Plan.***)
    - Ensure the people who are being transported to medical facilities are tracked and accounted for by the site team and HR.
    - Maintain Equifax's official list of victims and their status.
  - o Support victims and their families
    - Contact families of personnel that have been injured and provide them with all possible assistance, including assigning a liaison to the family of each seriously affected employee.
    - Determine need and scope of humanitarian support for affected personnel.
    - Provide financial support, emotional/psychological support and logistical support.
    - Engage Employee Assistance Program counselors as needed.
    - Coordinate (with Finance CAT member) any benefits or compensation dispensation related to personnel or their families.
    - Recommend to the CMT leader if a separate family gathering site needs to be established; coordinate with Facilities to get it set up.
  - o Expedite HR services
    - Review requests for critical staffing resources.
    - Coordinate medical clearance for all personnel expected to travel internationally.
    - Provide special assistance as needed with payroll processing, health and disability benefits, and all other benefits administration.

© 2016 Equifax, Inc. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000069

- Communicate status of personnel as appropriate:
  - Coordinate and track any communication with or notification of injured victims' families. DO NOT contact families of deceased personnel - law enforcement officials should perform next-of-kin notification.
  - If there are deceased personnel, coordinate with Security and/or local law enforcement to have an Equifax representative and a mental health professional present when next-of-kin notification occurs.
  - Monitor the medical condition of victims and to provide periodic updates to personnel (if available).
  - Oversee access to and confidentiality of information about staff or other personnel, as potentially required by authorities or Equifax response personnel.
  - If an international incident, establish dial-in telephone and electronic access to information for individuals outside the U.S.
  - Maintain primary point of contact with authorities (including hospitals, Red Cross, and others) regarding victims, their status and personal belongings.
  - Activate the employee information hotline (using both toll-free telephone numbers for in-bound calls from personnel or family members and Equifax's web site).
    - Ensure a plan is in place to keep this information up-to-date.
    - Work with Communications CMT member to determine appropriate scripts for those staffing the line.

© 2016 Equifax, Inc. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000070

Note: These action lists are not all-inclusive. Not all actions should be implemented in every situation. The action lists do not replace use of good judgment. Every situation will require additional actions based on the strategic and tactical requirements of the event.

C. Information Technology

- ❑ Participate in initial damage assessment when/if requested by the CMT or Facilities CAT.
- ❑ Review with CMT leader the appropriate IT CAT response level.
- ❑ Provides strategic IT leadership to the CMT.
- ❑ Review with CMT leader the appropriate IT CAT members to activate.
- ❑ Assemble IT CAT members, brief them, solicit recommendations and concerns, and establish a periodic review cycle to maintain collaboration between the CMT and the IT CAT.
- ❑ Recommend to CMT leader the actions needed to continue critical Equifax operation processes, agree on tasks and priorities.
- ❑ Contact the IT CAT to request the availability status of the technology infrastructure and the damage assessment. Provide summary information to the CMT. Maintain periodic updates based on established IT Operations procedures.
- ❑ Review the current situation status and recommend initial incident objectives to the CMT leader. Approve emergency IT expenditures.
- ❑ Assign priority tasks to IT CAT and establish process to monitor progress.
- ❑ Oversee implementation of the ***IT Disaster Recovery Plan.***
- ❑ Oversee implementation of the department's ***Business Continuity Plan.***
- ❑ Oversee IT CAT responsibilities:
  - o Oversee support of systems and telecommunications needs for CMT and all CATs.
  - o Work with Corp Communications to ensure Corporate Communications have the correct information involving IT incidents.
  - o Work with Incident Response Team/Communications to ensure all internal and external "Help Desk" personnel are familiar with the incident and how to respond to personnel questions.
  - o Manage all telephony issues. Reroute incoming calls to affected locations.
  - o Ensure IT CAT provides the tools that the CMT and all CATs need for communications such as active network access or ability to VPN from outside location.
  - o Work with HR to identify personnel needs for IT Disaster Recovery activities. Establish which personnel will be involved in DR activities and determine if they are available and prepared to engage when the DR activities begin.
  - o Approve and provide access to systems in the event authorized users are not available with the CMT or in any CAT.
  - o Perform system health checks and report/revolve any issues.
  - o Assess and coordinate repairs/replacement of computer hardware and software.
  - o Coordinate responses to cyber security issues with the Safety and Security CAT

© 2016 Equifax, Inc. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000071

Note: These action lists are not all-inclusive. Not all actions should be implemented in every situation. The action lists do not replace use of good judgment. Every situation will require additional actions based on the strategic and tactical requirements of the event.

D. Corporate Communications

- ❑ Review with CMT Leader the appropriate Communications CAT response level.
- ❑ Provides strategic communications leadership to the CMT.
- ❑ Activate the appropriate Communications CAT members.
- ❑ Determine need for involvement of outside PR resources; activate as needed.
- ❑ Assemble Communications CAT members, brief them, solicit recommendations and concerns, and establish a periodic review cycle to maintain collaboration between the CMT and the Communications CAT.
- ❑ Oversees media relations, coordination of messaging related to investor relations, internal Equifax communications.
- ❑ Monitor on-going news coverage of the event and communicate news information to the CMT leader.
- ❑ Assist CMT Leader in designating spokespersons; support spokesperson directly or through the Communications CAT.
- ❑ Evaluate and counsel the CMT leader on need for CMT leader or other senior management to go to the incident scene.
- ❑ Assign priority tasks to Communications CAT and establish process to monitor progress.
- ❑ Oversee implementation of the Equifax ***Crisis Communication Plan***
- ❑ Oversee implementation of the department's ***Business Continuity Plan.***
- ❑ Oversee Communications CAT responsibilities:
  - o Activate and staff the Crisis Communications Center (War Room) if not already active.
  - o Prepare draft "core press statement" and follow-up "press briefing statements" for review and approval by the CMT Leader and legal counsel.
  - o Respond to press inquiries. Establish a media briefing schedule. Publish media alerts.
  - o Consider need to secure services of a translation service.
  - o Prepare internal communications in conjunction with HR & Legal CATs.
  - o Assist HR in preparing and communicating event information to personnel globally.
  - o Obtain copies (video, audio, print, online) of all coverage and keep it indexed.
  - o Periodically update the communication strategy as necessary based on media reports.
  - o In conjunction with the IT CAT and other business CATs, contact all Equifax call centers to redirect crisis calls to the identified crisis response 800 number.
  - o If required, coordinate press briefings, including facility set-up in conjunction with the Office Facilities CAT
  - o Ensure that a communications coordinator is in place at the scene if necessary.
  - o Brief and coordinate with designated spokespeople at remote locations, if necessary.

© 2016 Equifax, Inc. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000072

Note: These action lists are not all-inclusive. Not all actions should be implemented in every situation. The action lists do not replace use of good judgment. Every situation will require additional actions based on the strategic and tactical requirements of the event.

E. Legal

- ❑ Take steps to make certain CMT and CAT meetings privileged, as deemed appropriate; including announcing to the CMT in the initial briefing that the Legal CMT Member is acting in a legal capacity providing legal advice to the team and all discussions are to be considered privileged. Attempt to do the same for critical CATs by providing a lawyer at each CAT meeting – Most critical are Communications and HR CATs.
- ❑ Review with CMT Leader the appropriate Legal Department CAT response level.
- ❑ Activate appropriate Legal Department CAT members, including outside counsel if required.
- ❑ Assemble Legal Department CAT members, brief them, solicit recommendations and concerns, and establish a periodic review cycle to maintain collaboration between the CMT and the Legal Department CAT.
- ❑ Assist the CMT Leader in evaluating the effects on the public.
- ❑ Recommend to CMT Leader the actions needed to continue critical Equifax legal operation processes, agree on tasks and priorities.
- ❑ Assess the need for Form 8-K and oversee preparation with Finance if necessary.
- ❑ Assess the need for NYSE, CFPB, State Attorney Generals (AGs), and/or Capitol Hill; contact and coordinate with Finance and Investor Relations personnel.
- ❑ Consider need to contact Board of Directors.
- ❑ Evaluate legal effects of incident on Equifax, and apprise CMT Leader on legal issues.
- ❑ Assign priority tasks to Legal CAT and establish process to monitor progress.
- ❑ Oversee implementation of the department's ***Business Continuity Plan.***
- ❑ Oversee Legal CAT responsibilities:
  - o Brief all personnel involved in the response about the correct way to capture and record information about the incident, with the issue of eventual discovery as the basis. Ensure this discussion occurs early in the response with the Administrative Support team keeping the official response log for the CMT, and consider providing full-time legal guidance to the documentation activities in the CMT.
  - o Maintain the official written record of Equifax's response and oversee records retention.
  - o Monitor the documentation of the incident and ensure information is being recorded in a way that will minimize liability, and being stored in a way that will facilitate discovery.
  - o Ensure all legally required notifications, fillings, and disclosures are made in a timely fashion.
  - o Oversee regulatory investigations.
  - o Oversee criminal investigations in conjunction with Security CAT.
  - o Manage forensic efforts to ensure evidence is being protected.
  - o Assess potential civil and criminal liability aspects of incident pertaining to Equifax and personnel – recommend legal representation when appropriate.

© 2016 Equifax, Inc. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000073

- Direct resolution of claims and assessment of liability against Equifax.
- Consider liability issues that may affect Equifax and/or its personnel.
- Review all potential actions being considered by Equifax and/or its agents, to ensure they adhere to U.S. and local laws and regulations.
- Remain aware of, and consider responses to any liability that may occur, due to injury or prosecution of any persons responsible for implementing corporate policy during a crisis.
- Prepare, at the end of a crisis, for the allegations being brought against Equifax by a person claiming to be affected by the event, shareholders, or a member of the public.
- Ensure all event documentary records are managed effectively. This includes determining who is permitted access to crisis-related Equifax information, how it is stored, and the proper form of ultimate disposal.
- Provide guidance to the affected site/business regarding preservation of evidence.
- Oversee and/or participate directly in incident investigations for significant events.
- Review and approve all final investigation reports.
- Assess other incidents in Equifax's history and within the industry, including compliance issues, and determine the likelihood of those issues being publicly connected to the current incident, communicate and provide legal advice and counsel to Communications as appropriate.

© 2016 Equifax, Inc. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000074

Note: These action lists are not all-inclusive. Not all actions should be implemented in every situation. The action lists do not replace use of good judgment. Every situation will require additional actions based on the strategic and tactical requirements of the event.

F. Finance

- ❑ Review with CMT Leader the appropriate Finance CAT response level.
- ❑ Activate the appropriate Finance CAT members.
- ❑ Assemble Finance CAT members, brief them, solicit recommendations and concerns, and establish a review cycle to maintain collaboration between the CMT and the Finance CAT.
- ❑ Recommend to CMT Leader the actions needed to continue critical Equifax operation processes, agree on tasks and priorities.
- ❑ Provide guidance to CMT and CATs regarding spending policies and procedures during the crisis.
- ❑ Review with CMT members specifics about insurance policies that may apply to the crisis.
- ❑ Oversee implementation of the department's ***Business Continuity Plan.***
- ❑ Oversee Finance CAT responsibilities:
  - o Assign priority tasks to Finance CAT and establish process to monitor progress.
  - o Review insurance coverage that may apply to the crisis and contact providers. File any required notices of claims or other documents.
  - o Work with insurance provider's claims representatives to help establish timely responses to all affected stakeholders, especially those who may tend to take legal action against Equifax, e.g., businesses that lost business or injured community members.
  - o Establish a method to isolate and collect costs related to the incident. Focus on preparing substantiation for insurance claims.
  - o Insure adequate business controls are in place during the crisis.
  - o Establish SEC or other financial regulatory notification if required.
  - o Ensure access to cash and/or credit lines as needed.
  - o Assess potential to effect credit ratings – access to credit.
  - o Establish a proactive program to communicate to analysts and investors.
  - o Determine disbursement capabilities and needs.
  - o Coordinate (with Human Resources) any benefits or compensation dispensation related to personnel or their families.
  - o Maintain records of travel costs associated with the incident.

© 2016 Equifax, Inc. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000075

Note: These action lists are not all-inclusive. Not all actions should be implemented in every situation. The action lists do not replace use of good judgment. Every situation will require additional actions based on the strategic and tactical requirements of the event.

G. Global Operations

- ❑ Review with CMT Leader the appropriate Global Operations CAT response level.
- ❑ Activate the appropriate Global Operations CAT members.
- ❑ Assemble Global Operations CAT members, brief them, solicit recommendations and concerns, begin deployment of Business Continuity Plans as needed and establish a periodic review cycle to maintain collaboration between the CMT and the Business Operations CAT.
- ❑ Recommend to CMT Leader the actions needed to continue critical Equifax operation processes, agree on tasks and priorities.
- ❑ Assess the client service operations and provide recommendations to the CMT if operations have been affected. Oversee the timely recovery of client service operations.
- ❑ Evaluate the potential financial effects of the disruption and provide an assessment to the CMT. If needed, determine the requirements for prioritizing services.
- ❑ Oversee implementation of the department's ***Business Continuity Plan.***
- ❑ Oversee Global Operations CAT responsibilities:
  - o Review/inform the known extent of the crisis as it impacts operations to include:
    - Personnel
    - Facility
    - Customer
    - Vendor/Partner
    - Processing Capability
  - o Assign priority tasks to Global Operations CAT and establish process to monitor progress.
  - o Establish contact with the key sales and operations leader(s) at the affected site(s) and obtain initial conditions and support needs. Assist in contacting other client support centers to redirect crisis calls per direction from the CMT.
  - o Evaluate the situation to determine if the disruption will compromise the ability to conduct and support business, for what period and which areas of operations would be impacted by the disruption.
  - o Assess potential for the incident to affect other operations. Those operations potentially affected have been given situational guidance, e.g., shut down, close the branch or increase preparedness. If required, ensure regulatory notification of closing occurs.
  - o Communicate with external service providers to ensure safe, orderly services exist as the locations can handle them.
  - o Work with the Corporate Communications CAT to develop internal and external communications.
  - o Work with third party suppliers to ensure cooperation if the crisis involves their personnel or locations.

© 2016 Equifax, Inc. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000076

- Ensure client service representatives have accurate information about the incident and have a scripted response to client questions created in conjunction with the Communications CAT.
- Coordinate on labor management and vendor management to address any high inbound call volumes.

© 2016 Equifax, Inc. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC.

Note: These action lists are not all-inclusive. Not all actions should be implemented in every situation. The action lists do not replace use of good judgment. Every situation will require additional actions based on the strategic and tactical requirements of the event.

H. Safety and Security

- ❑ Review with CMT Leader the appropriate Safety and Security CAT response level.
- ❑ Activate the appropriate Safety and Security CAT members.
- ❑ Assemble Safety and Security CAT members, brief them, solicit recommendations and concerns, and establish a periodic review cycle to maintain collaboration between the CMT and the Safety and Security CAT.
- ❑ Recommend to CMT Leader the actions needed to continue critical Equifax operation processes, agree on tasks and priorities.
- ❑ Oversee implementation of the department's ***Business Continuity Plan.***
- ❑ Oversee implementation of ***Equifax Security Incident Handling Policy & Procedures***
- ❑ Oversee Safety and Security CAT responsibilities:
  - o Assign priority tasks to Safety and Security CAT and establish process to monitor progress.
  - o Establish contact with the Safety and Security manager or alternate at the affected site to determine initial conditions and support needs.
  - o Assess the life safety effects of the crisis. An initial evaluation of the life safety and security risks both on and off site should be performed and a periodic review schedule should be established to ensure effective monitoring of the situation.
  - o Ensure that site emergency responders managing the safety of personnel and general public and are operating in conjunction with local emergency officials.
  - o Assess the need for external providers, e.g., guard services, and if needed, hire them and have them operate under the direction of the Safety and Security CAT.
  - o Ensure that law enforcement agencies are identified, a dialog with each agency is established.
  - o Ensure Security personnel are assisting HR to account for all personnel and locating those that cannot be accounted for.
  - o Deploy security measures for the CEO and CMT Members as appropriate.
  - o Assess and establish additional security controls for the Command Center if necessary.
  - o Provide security for senior management that may be traveling to the site.
  - o Coordinate responses to cyber security issues with the Information Technology CAT and external providers.
  - o Coordinate with Corporate Communications to provide Safety and Security incident information.
  - o Maintain Card Brand Notification procedures.

© 2016 Equifax, Inc. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000078

Note: These action lists are not all-inclusive. Not all actions should be implemented in every situation. The action lists do not replace use of good judgment. Every situation will require additional actions based on the strategic and tactical requirements of the event.

I. Real Estate

- ❑ In conjunction with Safety and Security CAT, approve all assembly points for CMT and CATs to make sure they are safe.
- ❑ Review with CMT Leader the appropriate Facilities CAT response level.
- ❑ Review the appropriate response level for any other affected office facilities.
- ❑ Activate the appropriate CAT members.
- ❑ Assemble Office Facilities CAT members, brief them, solicit recommendations and concerns, and establish a periodic review cycle to maintain collaboration between the CMT and the Office Facilities CAT.
- ❑ Recommend to CMT Leader the actions needed to continue critical Equifax operation processes, agree on tasks and priorities.
- ❑ Receive information from the affected office emergency response team and use it to provide recommendations to the CMT.
- ❑ Oversee implementation of the department's ***Business Continuity Plan.***
- ❑ Oversee Facilities/Travel/Procurement CAT responsibilities:
  - o Assign priority tasks to Office Facilities CAT and establish process to monitor progress.
  - o Set up the Crisis Command Center to support the CMT and CAT facilities and logistics.
  - o Link up any available news broadcasts from the area or location of crisis by providing television viewing capabilities where the CMT is meeting.
  - o Assess facility resources and office equipment needs in coordination with IT.
  - o Assist in recovery planning as appropriate.
  - o If needed, ensure transportation for those who have special needs to get them to off-site locations is provided.
  - o If appropriate, designate an Office Facilities liaison to the police or fire department on-site command post and review security tapes with Safety and Security CAT.
  - o Expedite procurement of any goods or services needed by the CMT or CATs.
  - o Evaluate contractual relationships between Equifax and suppliers with legal to determine if force majeure may have to be declared.
  - o Work with HR CAT to help account for people by providing travel itineraries for personnel who are traveling during the event.
  - o Work with HR CAT to help account for any people at an effected location by providing floor plans/seating locations as appropriate.
  - o Work with carriers to compare personnel travel itineraries with carrier manifests to confirm personnel are actually traveling, and provide information to the HR CAT.
  - o Provide priority travel services to CMT and CAT members that need to travel in response to the crisis, including charter air and ground transportation.
  - o Maintain records of travel costs associated with the incident.

© 2016 Equifax, Inc. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000079

Note: These action lists are not all-inclusive. Not all actions should be implemented in every situation. The action lists do not replace use of good judgment. Every situation will require additional actions based on the strategic and tactical requirements of the event.

J. Marketing/Analytics/Data Services

- ❑ Review with CMT Leader the appropriate Marketing, Analytics & Data Services CAT response level.
- ❑ Activate the appropriate Marketing CAT members.
- ❑ Assemble Marketing CAT members, brief them, solicit recommendations and concerns, and establish a periodic review cycle to maintain collaboration between the CMT and the Marketing, Analytics & Data Services CAT.
- ❑ Recommend to CMT Leader the actions needed to continue critical Equifax operation processes, agree on tasks and priorities.
- ❑ Evaluate the financial effects of the crisis and communicate to CMT.
- ❑ Oversee implementation of the department's ***Business Continuity Plan.***
- ❑ Oversee Marketing, Analytics & Data Services CAT responsibilities:
  - o Assign priority tasks to Marketing CAT and establish process to monitor progress.
  - o Identify key products and partners (channel, and third party) that may be affected, and provide list to Business Units.
  - o Establish a daily product & services availability review schedule together with Business Operations.
  - o Work with Corporate Communications, Global Operations, Legal and Finance CATs to establish priorities under reflection of contractual obligations and obtain a plan for product availability.
  - o Establish a recovery schedule that is regularly updated and reviewed as a basis for ongoing communications with clients.
  - o Work with Legal CAT to determine impact of Service Level Agreements (SLAs)

© 2016 Equifax, Inc. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000080

Note: These action lists are not all-inclusive. Not all actions should be implemented in every situation. The action lists do not replace use of good judgment. Every situation will require additional actions based on the strategic and tactical requirements of the event.

K. Business Units

(International, Corporate Development, GCS, USIS, Workforce Solutions)

- ❑ Review with CMT Leader the appropriate BU CAT response level.
- ❑ Activate the appropriate BU CAT members.
- ❑ Assemble BU CAT members, brief them, solicit recommendations and concerns, and establish a periodic review cycle to maintain collaboration between the CMT and the BU CAT.
- ❑ Recommend to CMT Leader the actions needed to continue critical Equifax operation processes, agree on tasks and priorities.
- ❑ Evaluate personnel and the financial effects of the crisis and communicate to CMT.
- ❑ Oversee implementation of the department's ***Business Continuity Plan.***
- ❑ Oversee BU CAT responsibilities:
  - o Assign priority tasks to BU CAT and establish process to monitor progress.
  - o Identify employees, key products and clients that may be affected, and prepare list of contacts.
  - o Evaluate effects of the event on direct and indirect clients.
  - o Coordinate a proactive communications program to inform clients of the status of their accounts and other important information. Make sure to respect contractual obligations, consult with legal as needed.
  - o In conjunction with the Legal CAT, understand all contractual obligations. Assess risk of Service Level Agreement (SLA) contract violations.
  - o Establish a daily product & services availability review schedule together with Business Operations.
  - o Communicate to clients when information is available and as directed by CMT and CMT CAT. In no case speculate or promise solutions to clients.
  - o Evaluate contractual relationships with clients (with legal, operations and financial input) and determine if force majeure should be initiated and prepare plans and communications relative to those processes. Submit plan to CMT for approval.
  - o Work with Global Operations, Legal and Finance CATs to establish priorities under reflection of contractual obligations and obtain a plan for product availability.
  - o Establish a recovery schedule that is regularly updated and reviewed as a basis for ongoing communications with clients.
  - o Communicate to employees, partners, and customers when back to normal operations.

© 2016 Equifax, Inc. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000081

Additional Actions

Corporate Development	• If there is a crisis during advanced stages of an acquisition, notify the CM team if there are risks of losing the transaction. • If there is no current M&A activity, determine if this will be suspended until the crisis has concluded or has been stabilized to a satisfactory level. • Work with Security CAT to determine if international security measures need to be increased.
International	• Contact GMs for local events and engage with regional CAT. • Work with regional CAT to determine business impact.
GCS	• Coordinate with Global Operations to determine if any impact to call centers.
USIS	• Determine if USIS personnel can be redeployed to other critical support duties. • Determine if the Small Business Financial Exchange (SBFE) needs to be contacted.
Workforce Solutions	• No additional activities/actions noted.

© 2016 Equifax, Inc. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000082

IV. Revision History

Date	Name	Version	Description of Changes
5/2013	Mike Douglas	1.0	Initial version of document
9/2013	Mike Douglas	1.1	Revisions
10/2014	Mike Douglas	2.0	Annual Update and Revisions
4/2015	Mike Douglas	3.0	Annual Update and Revisions
6/2016	Mike Douglas	4.0	Annual Update and Revisions

© 2016 Equifax, Inc. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000083

EQUIFAX, INC., "CORPORATE CRISIS MANAGEMENT PROGRAM, APPENDIX H"

EQUIFAX

Corporate Crisis Management Program

Appendix H

Security and Safety

Crisis Action Team Plan

August 2016

Version 4.0

The Security CAT can be activated through the Equifax Notification System or via call tree. Activation should be initiated by CAT Leader or Alternate.	
Primary Security CAT Assembly Point	Fusion Center Conference Room
Secondary Security CAT Assembly Point	Bond Conference Room
Conference Bridge Line	Number: 1-866-398-2885 Participant Code: Redacted Host Code: Redacted

Table of Contents

Security Crisis Action Team Plan

During a Response, use the "Action List" beginning on page 13.

Purpose

The Security Incident Response and Crisis Action Team ("CAT") Plan defines principles, roles and responsibilities for team members who support the physical, cyber security and life safety aspects of Equifax's incident response program. This team is known as the Security CAT.

This plan is not intended to stand alone; it is used to support the ***Equifax Crisis Management Plan*** (***"CMP"***) , the Equifax Crisis Management Team ("CMT") and the Security Incident Response Procedures Guide. All Security CAT members must be familiar with the details of the ***CMP***.

This plan provides a "Potential Considerations List" for Security CAT members and is designed to ensure a consistent, collaborative response during an event by all active CATs.

The Security CAT is activated by the CMT leader or the Security CMT member. It will be implemented in context of the ***CMP***. The responsibilities of the Security CMT member are listed in ***Table A*** of the ***CMP***.

Crisis Management Principles

Scope: The Security CAT scope is typically limited to the Security Department's response to an incident that has been declared a corporate incident or a corporate crisis by the CMT. However, the Security CAT may also be activated by the Security organization for its own purposes, if appropriate.

Focus: The primary focus of the Security CAT is on the physical and executive security, information security and personnel safety elements of an incident and on issues that cut across departmental lines. The Security CAT will also support or consult with the affected departments and offer specialized resources available at the corporate level.

External Resources: The Security CAT may require additional resources beyond those within the company. In all cases of external resources, the resources will be considered part of the Security CAT and will operate under the direction of the CMT member – Security.

Operational Guidance: The Security CAT will use the Potential Considerations List in Section D to manage the Security Department response. Please note that all actions on the list may not be appropriate in every incident, nor are these the only actions required for a successful response. In all cases, judgment should be used to determine the correct actions.

© 2016 Equifax. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC.

Crisis - Definition

A crisis is an unplanned event related to Equifax's business that has the potential to:

- Present a significant threat to human health, safety or the environment.
- Cause a significant adverse effect on Equifax's reputation.
- Cause a significant disruption to Equifax's business.

Notwithstanding the definition above, a crisis is any event identified as such by the CAT Leader or designate.

Examples of potential Equifax crises include:

- Operational issues such as office/data center emergencies.
- Any situation that attracts the attention of the media and the public and could damage the reputation of Equifax.
- Natural disasters such as hurricanes, earthquakes, flooding
- Public health disasters, epidemics or pandemics.
- Financial crises, such as significant market-related situations, a major decline in earnings, or fraud.
- Informational crises, such as a loss of proprietary and confidential information, tampering with computer records, security incident or loss of IT infrastructure.
- Legal issues, such as the indictment or arrest of a senior executive.
- Political/Civil unrest impacting business operations or personnel.
- Loss of the use of major offices /data centers for any other reason.

The Security CAT is activated when the CAT Leader (or designate) decides an event meets or has the potential to meet the definition above. Further information on activation procedures is provided in **Activation Framework Overview.**

© 2016 Equifax. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000087

Activation Framework Overview

Phase 1: Assess the Situation & Assemble the TeamEvent reported to Incident Assessment Coordinator for activation assessment.

The Incident Assessment Coordinator will assess the threat, seek guidance from other leadership if needed (Regional GM, BU Heads), and then determine the level of CAT activation required. The Incident Assessment Coordinator is notified via the Security Desk and/or a member of the Equifax Management Team and includes:

Dodd Williams Michael Douglas Susan Mauldin

Before activating the Regional CAT, the Incident Assessment Coordinator will decide on an appropriate activation level based on the specific circumstances of the incident. The level can escalate as necessary to acquire resources for crisis response. All serious incidents must be reported to the CAT Leader or designee immediately. If there is any doubt about the activation level, the Regional CAT should be, at a minimum, activated at the **Notify Only Level**.

Activation Level Decision: No Action, Notify Only, Stand-by, Respond.

Notify Only Level
The CAT is notified when an incident is not an obvious Equifax crisis initially, but which warrants monitoring or would be of interest to members of the CAT. At this level, **CAT Members DO NOT respond or assemble**. Members are typically informed of the event during normal hours, typically via e-mail, and the Incident Assessment Coordinator becomes responsible for tracking incident status.

Stand-by Level
The Regional CAT may be put on "Stand-by" when an incident has the potential to become a Equifax crisis but CAT assembly is not yet appropriate. During this stage, CAT members will be notified of the incident and placed on notice that the team may be activated in the future. CAT members should then be making the appropriate arrangements to ensure the CAT is staffed for their function. **CAT Members DO NOT assemble at the Stand-by level.**

Respond Level
The Regional CAT will be activated when there is a high potential for a Equifax crisis to occur. The activation can occur immediately upon initial notification or as an event escalates from a lower activation level. All CAT members will be notified of the incident and be asked to attend an initial briefing. Declaring "Respond-level" activation immediately invokes the Regional Crisis Action Plan. Regional CAT activation will typically use the Mass Notification System.

© 2016 Equifax. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000088

Communicate to the Security CAT if needed.

In all situations when the Incident Assessment Coordinator has determined the incident warrants CAT activation at any level, CAT members will be notified as described above. If the CAT is assembled, the Mass Notification System will be activated and simultaneous communication to all CAT members and alternate members will occur. All documented contact points will be involved (Office Phone, Cell Phone, Home Phone, E-mail, etc.). In most cases, a conference line will be provided as part of the activation process.

Only proceed to Phase 2 if a RESPOND level activation is declared.

Phase 2: Prepare to conduct the Initial Briefing

- Collect information.
- Prepare agenda (next page).

Phase 3: Conduct the Initial Briefing (For all CMT members and alternates–usually a call)

- Brief team.
- Discuss actions that are required immediately.
- Specify next meeting time/location.
- Discuss CAT activation.
- Activate CATs and review situation. Get CAT input.

Phase 4 Conduct second meeting (CAT assembles)

- Use pre-determined agenda (next page).
- Status report from affected site/business.
- Status reports from each function (include information from CAT briefings).

Phase 5 Continue Response Activities

- Conduct routine meetings using Brief, Discuss, Action model.
- Continue management of crisis.

Phase 6 Conclude the crisis response (Recovery)

- Stand down CAT – move into recovery stage.
- Assign responsibility for on-going management efforts.
- Charter incident investigation team as necessary.
- Conduct After Action Review.

© 2016 Equifax. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000089

Initial Actions – Respond Level Activation

Review Guiding Principles and Priorities:

1. Place the highest priority on Life Safety – the welfare of all people including personnel, clients, visitors, emergency responders and community members.
2. Protect our assets and preserve our ability to operate and supply our clients.
3. Maintain a strong Equifax reputation through ethically and socially aware behaviors that ultimately preserve shareholder value.

AFTER Declaring an Activation

Initial Notification

- Receive briefing from Incident Assessment Coordinator.
- Confirm decision to activate CAT.
- Confirm plan for initial CAT briefing.
  - Time, location, call-in numbers, etc.
- Consider the need to inform the International Crisis Action Team or Corporate Crisis Management Team.
- Consider the need to inform any UK regulatory agencies.

Prepare for initial CAT briefing

- Review the Initial CAT Briefing Agenda (below) to confirm responsibilities.
- If possible, obtain an updated status of the incident.
- Consider the timing for the first full CAT meeting.

Agenda Topic	Desired Outcomes
Purpose of the call	Brief the Team. Direct Admin Support member to document all facts and decisions.
Identify all callers	Document all callers and ensure all CAT roles are represented.
Situation Description	Provide the current details of the situation to the CAT.
Support	Identify support requested by the site or business. Discuss the potential additional support the CAT may be required to provide.
Team Selection	Identify the team members (name and role) that will continue to support this event.
Communications	Determine what communications have been made and what communications are still required. Assign responsibilities.
Logistics	Announce next meeting time and location (meeting room and telephone numbers).
Adjourn meeting	Final concerns issues. Direct CAT members to assemble, brief and provide direction to his or her support team.

© 2016 Equifax. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000090

Team Membership and Responsibilities

The Security CAT identifies primary members and alternate members to provide the ability to respond to an incident around-the-clock. The relationship between the CMT and Security CAT is shown on the chart in the following section. Security CAT membership comprises the following disciplines:

Role	Primary	Alternate
CMT Member	Susan Mauldin	Doug Steelman
CAT Leader	Dodd Williams	Matt Modica
Incident Manager	Michael Douglas	Dodd Williams
Life Safety/Physical Security	Matt Hyman	Sheree Franklin
Cyber Threat Center	Doug Steelman	Francis Finley
Investigations	Greg Baker	Mark "Tony" Alig
Security Engineering	Diab Hitti	Andrew Gingher
Corporate Communications	Dianne Bernez	TBD
Legal	Troy Kubes	Julia Houston

The team members are available to assemble in the **Fusion Center Conference** as a primary location or participate via teleconference as needed in response to a crisis.

The primary roles and responsibilities of the Security CAT are listed below:

- Serves as principal Security & Life Safety advisor to the CMT.
- Manages and directs Security & Life Safety resources.
- Approves the safety and security of any location where the CMT and CATs may assemble PRIOR to assembling the teams.
- Assures the assembly locations remain safe and secure for the duration of the response.
- Assess threats to executive members' personal residences and takes needed action to protect them.
- Insures all needed Information Security actions are taken to protect confidential data and to prevent unauthorized access or use of Equifax system or data.
  - Stop unauthorized access or disclosure of confidential data.
  - Limit immediate incident impact within the Equifax IT environment.
  - Participate in Root Cause Analysis
  - Ensure existing policies and standards are followed and updated in order to prevent further cyber related attacks.

© 2016 Equifax. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC.
EFXCONG-SBC000000091

- Acts as a resource to local responders regarding all Security & Safety aspects, including deployment of site Emergency Response plans.
- Oversees reporting of physical, medical, and cyber related incidents to governmental authorities, in conjunction with affected sites.
- Works with CMT to comply with regulatory investigations and recommendations.
- Serves as primary CMT law enforcement liaison.
- Preserve physical/forensic evidence
- Manages and directs security resources for corporate offices.
- Manages executive security and site security globally.
- Assures safety of executives in route to and at incident scene.
- Provides functional expertise, as needed, in a kidnapping or hostage situation.
- Arranges for 24/7 personal security for any executives. Providing liaison and coordination with appropriate law enforcement agencies and specialized security consultants, as directed by the CMT.
- Ensures all official documents are properly controlled and handled as potential evidence (as directed by Legal), which may be required to assist in investigations.
- Advises CMT about access control practices for Equifax property for affected locations.
- Coordinates information security activities with the Information Technology CMT member.
- Oversees the affected site's ***Emergency Response Plan.***
- Oversees the ***Security Incident Response Procedures Guide***
- Activates and oversees the department's ***Business Continuity Plans.***

The Security CAT should provide expertise in the following areas:

- Operation of the various security centers and equipment.
- Relationships with law enforcement organizations.
- Relationships with third-party providers and consultants.
- Executive security.
- Site security.
- Criminal investigations (Personal/Property crime).
- Knowledge of staffing and facility configuration planning.
- Life safety and industrial and occupational safety and health.
- Network Security and Security Engineering
- Information security Incident Handling, Cyber-threat Analysis, and Forensics

© 2016 Equifax. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000092

Incident Definition and Declaration

An incident is the act of violating an explicit or implied security policy. The types of activity that are widely recognized as being security incidents are violations categorized as, but are not limited to, attempts (either failed or successful) to gain unauthorized access to a system or EFX data, unwanted disruption or denial of service, the unauthorized use of a system for the processing or storage of data, or changes to system hardware, firmware or software characteristics without the owner's knowledge, instructions, and approval.

The level of consequence of an incident refers to the relative impact it has on an organization. The types of impact include: loss of data; the loss or theft of information, IT resources, revenue or confidence in an EFX company or mission area by the general public or customers; or a high level of damage that must be corrected prior to system restoration.

Within the Cyber Threat Center, security incidents shall be declared for the following reasons:

- Analysis of monitoring system reports that show signs of system compromises in the logs;
- Notification by an external entity of an EFX IP or e-mail addresses being the cause or victim of malicious or questionable activity;
- Alert, notification, or warning from other business partners, customers or departments that an EFX IP address(s) is the target or originator of malicious activity;
- Complaints by an Internet Service Provider (ISP) that detail specific, prohibited activities by an EFX host, IP address or e-mail address;
- Floods of viruses, worms and Trojan Horses for which anti-malicious code/anti-virus software is not available. In attacks where the attack vector and exploit code is similar/identical, one EFX incident number will be assigned for the entire process;
- Complaints from the public, or other employees that include specific examples or references of inappropriate or illegal use by EFX employees, cooperators, partners or contractors utilizing EFX IT; and
- A self-discovery by an EFX organization that meets the definition of an incident (i.e., virus discoveries, policy violations, criminal actions, etc.)

© 2016 Equifax. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC.

Security Incident Classification

Security incidents are declared when they are serious and considered major in nature. Declarations and classification will be based on an initial risk assessment of the situation including: number of affected systems; network impact; business services impact; sensitivity of information threatened or compromised, and the potential for harm to EFX (e.g. financial, service, sales, customer trust, or Equifax image impacts). Outlined below are criteria for security incidents:

Note: All Cyber specific incidents only Medium (SEVERE) and above will generate notification to the Security CAT.

High (CRITICAL) incidents are events that involve compromise of Equifax systems or data, often involving multiple systems or data records or pose an immediate threat to facilities or employees. These incidents will be handled immediately and operate on a strict need-to-know distribution. Examples of CRITICAL incidents include:

- Recurring SEVERE incident;
- Threats posing eminent threat to facility or employees;
- Employee/contractor attempting to send Equifax Confidential data to an external personal email account/online storage or other external entity;
- Phishing attack against Equifax;
- Malicious data access and/or alteration by employee or contractor;
- Unauthorized access to data or systems, accidental or malicious;
- Hijacking of Equifax domains;
- Confirmed computer, network or application compromise;
- Disclosure, loss or corruption of critical data;
- Malicious files found on critical system;
- EFX website defacements or compromises;
- Successful DDoS attacks by EFX systems or against EFX systems;
- Unauthorized use of a production system for processing or storing non-EFX or prohibited data or information; and
- Any violation of any local, state, federal or international law.

Medium (SEVERE) level Security Incidents are potentially serious events involved a critical asset with moderate damage and should be handled within eight (8) hours after the event occurs or notification of the event is made to the EFX Global Cyber Threat Center. This would include inappropriate access to confidential data by an Equifax customer, vendor or other known third party.

- Recurring WARNING incident;
- Changes to system hardware, firmware or software without the system owner's authorization;
- Connection of unauthorized wireless access device to company network(s);
- A contractor or employee errantly or maliciously attempts to transfer Confidential data outside of the Equifax network in an unapproved manner;

© 2016 Equifax. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000094

- Abuse of resources impacting critical systems or services;
- Attempts to circumvent Equifax Security Controls;
- Misuse of company property, facilities or services including accepting payment or services to provide access to or use of EFX IT resources in excess of one's authority, such as forwarding spam, engaging in unofficial/unauthorized chat, non-EFX e-mail and instant messaging services; and
- Discovery of risk that could become CRITICAL.

Low (WARNING) level Security Incidents involved non-critical assets and little damage. They should be handled within 24 hours after the event occurs or notification of the event is made to the EFX Global Cyber Threat Center.

- Recurring INFORMATIONAL incident;
- Employee/contractor who violates Equifax Data Classification policy through DLP violations inclusive of low volumes of data destined for a business;
- IPS reports that define activity as medium or unsuccessful system intrusion attempt;
- Unauthorized use of a system for processing or storing EFX data;
- Installation, use or sharing of unauthorized software;
- Unconfirmed computer virus/worms (depending on impact to department and if the infection is the result of a security policy violation);
- Undocumented or unapproved vulnerability scans;
- Isolated virus outbreaks; and
- Discovery of risk that could become SEVERE

Other types of incidents are categorized as adverse security events and shall not be declared security incidents unless there is a confirmed compromise of sensitive information, a threat to EFX data or subsequent escalation to a security Incident.

Evidence Handling Procedures

All evidence should be processed according to the evident handling procedures outlined in the Security Incident Response Procedures Guide. EFX follows current industry best practices for handling and securing digital evidence, and the procedure guide is periodically updated reflect these practices. These procedures and guidelines, while covering the most common areas of evidence handling, are neither all-inclusive nor a mandate, as each investigation may require a unique approach as agreed upon by all parties.

© 2016 Equifax. All Rights Reserved

Security CAT – Action List

Please note that all actions in the list may not be appropriate in every incident, nor are these the only actions required for a successful response. In all cases, judgment should be used to determine the correct actions.

Initial Actions and Assigning Resources (CAT leader)

[] 1. Advise senior management of incident and reaffirm responsibilities. Review roles of Security management and staff.

[] 2. Activate the Security CAT and confirm meeting location.

[] 3. Review the need for outside suppliers. If needed, employ outside suppliers and have them operate under the direction of the Security CAT.

[] 4. Assign a resource to account for all Security Department employees, contractors and guests and report any missing, injured or unaccounted people to the assigned HR resource (See item # 6 and see additional guidance in Section E.)

[] 5. Assign a resource to maintain information flow among the CMT, all other CATs, affected departments, and outside suppliers.

[] 6. Establish and communicate to Security CAT a method to capture action log and retain notes for post incident review.

[] 7. Activate additional Security staff as needed and assign tasks.

CAT Considerations

Physical Security Aspects

[] 8. Brief Site security personnel and reception if appropriate.

[] 9. Obtain report from Security and Emergency Management and report to CMT regarding response details:

- Number and status of victims
- Victim transport – which hospitals?
- Law enforcement involvement
- Evacuation status (if applicable)
- Access to building and property
- Immediately identified damage

© 2016 Equifax. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC.

[] 10. Assist HR to account for all people including staff, contractors and visitors. Each department will be responsible for their own staff and report findings to HR. HR will need information from Security and Facilities to aid in the search. Some data that they may need includes:

- Security badge data
- Visitors lists from front desk
- Hospital transport information as known

[] 11. Prepare and submit a security plan for the CMT Command Center and other critical facilities to the CMT leader.

[] 12. Initiate enhanced security procedures at all sites. Access control and security procedures elevated throughout the corporation as necessary.

[] 13. Receive and distribute to security personnel official company statement(s) from Communications CAT.

[] 14. Determine if CMT and CATs relocation is needed.

[] 15. Provide Security liaison to Municipal Authorities and liaisons to Fire/Police Incident Command Post as needed at the Emergency Operations Center. Work with Police for site and criminal issues (in conjunction with Legal). Be prepared to supply video, floor plans and other building information as appropriate.

[] 16. Contact outside service providers (Guard service, private investigators, law enforcement specialists, etc.) to alert them to the emergency and the potential need for assistance. Evaluate the provider(s) ability to quickly mobilize adequate resources upon request.

[] 17. Review and approve requests for additional security resources for locations throughout Equifax. This would include alerting security resources (Guard service, private investigators, Law enforcement specialists, etc.) of the emergency and potential need for assistance. Evaluate the provider(s) ability to quickly mobilize adequate resources upon request.

[] 18. Recommend that all other CATs provide a list of the authorized/restricted employees and contractors for the alternate worksite. Provide copy of list to Security CAT team for relocation efforts.

[] 19. Provide security advice and consultation for personnel traveling to the affected site.

[] 20. Provide executive protection for all potential threats to personnel.

[] 21. Continuously evaluate and mitigate threats, including threats to affected site and other company facilities.

[] 22. Provide frequent status updates to the CMT members and other CAT teams.

[] 23. Oversee the ***Security BC Plan***.

© 2016 Equifax. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC.
EFXCONG-SBC000000097

Cyber Threat Center

[] 24. Monitor network security to prevent unauthorized access by former employees, media, etc.

[] 25. Contact security engineering for any additional resources and/or assistance.

[] 26. Monitoring of unauthorized access attempts, inappropriate usage, denial of service and other suspicious and/or malicious activity.

[] 27. Distribution of security advisories.

[] 28. Centralized reporting of forensic reports.

[] 29. Performing vulnerability assessments.

[] 30. Provide user awareness and training.

[] 31. Coordination of disparate threats within a single monitoring group providing intelligent response services for the global Equifax enterprise.

[] 32. Determine if system breach has impacted PCI-related data and review incident response notification procedures outlined in the ***Equifax Crisis Management Plan, Appendix A, "Notification and Activation Procedure"***.

Deactivation and Post Incident Actions

Conducting a lessons learned post mortem meeting addressing the following questions, and any others that arise is a critical part of the Incident Response process. Such meetings allow Incident Response Team members to address that drive improvements in all previous Incident Response Phases.

[] 33. Coordinate and disseminate "Return to Normal" message to employees, vendors, contractors, and other stakeholders.

[] 34. Compile all documented activities in incident status report. Collect and retain all notes and logs created during the event for later post-incident review.

[] 35. Deactivate IT CAT and all response vendors as appropriate.

[] 36. Participate in debriefing sessions as directed by the IRT and/or CMT.

- How well did staff and management perform in dealing with the incident? Were the documented procedures followed? Were they adequate?
- What information was needed sooner?
- Were any steps or actions taken that might have inhibited the recovery?
- What would the staff and management do differently the next time a similar incident occurs?

© 2016 Equifax. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC.

- What corrective actions can prevent similar incidents in the future?
- What additional tools or resources are needed to detect, analyze, and mitigate future incidents?
- Additionally, a follow-up report should be created for the management and extended team(s) as described below:
  - Prepare a report for Equifax Executive Management to include:
  - Estimate of damage/impact;
  - Action taken during the incident (not technical detail);
  - Follow on efforts needed to eliminate or mitigate the vulnerability;
  - Policies or procedures that require updating; and
  - Efforts taken to minimize liabilities or negative exposure.
  - Provide the chronological log and any system audit logs requested by the Extended Team.
  - Document lessons learned and modify the Incident Response Plan accordingly.

Legal and Finance work with the local authorities as appropriate in the case that the incident; and HR and Corp. Security work with Equifax management to determine disciplinary action in the case that the incident was from an internal source

© 2016 Equifax. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000099

Security for People Guidance

The HR CAT is responsible for compiling all data about the status of people during a crisis; however, each Departmental CAT is responsible for reaching out to their department's line organization or other resources to help account for their staff.

1. **Once safely out of the area of danger, assign a resource to track department staff status information.** Ideally, this person should not be member of your CAT, but another person who does not have another emergency management or crisis management role.

2. **If assembled physically, write down the names of people you know to be safe and the ones you cannot account for (within vicinity).** If you have evacuated, this may be chaotic, but write down as many names as possible. Ask employees if they know anyone to have been injured as well as any staff members that they know were not in the area of the incident (such as on vacation, traveling, etc.)

3. **Through chain of command within department, ask managers call out to check on employees and send results to assigned resource.** Ask managers to track their information and provide a summary to you at a regular interval (daily, every 3 hours, etc.)

4. **For identified injured employees, notify the HR CAT immediately!** Try to get additional information as possible about the location of the victim. Always document the source of information. What hospital? Has the family been notified?

5. **As possible, account for any contractors and guests and send to the HR CAT.**

6. **Do not contact families or conduct Next-of-kin notifications.** The HR CAT will coordinate all family notifications. Remember that some of the information collected in the immediate aftermath of an incident may be incorrect. If you have home numbers and are attempting to reach out to employees, be prepared to talk to family members. Calmly inform them that an incident has occurred. Instruct them to call back or have their family member call back when they see them. Do not speculate. Do not provide incident details, but be polite and compassionate.

7. **Accounting for people takes time. Keep HR regularly updated on your efforts.**

Send all of your information to the HR CAT. Within the first hours of the response, the HR CAT will reach out your CAT to provide a method to receive your information. If you do not hear from the HR CAT, send your information to EFXpeoplewatch@equifax.com

Keep the HR CAT updated regularly on your efforts. Accounting for people takes time!

© 2016 Equifax. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC.

Revision History

Date	Name	Version	Description of Changes
4/2013	Mike Douglas	1.0	Initial version of document
6/2013	Mike Douglas	1.1	Plan revisions
10/2013	Mike Douglas	1.2	Plan revisions
1/2014	Mike Douglas	2.0	Annual update
3/2014	Adam Fletcher	2.1	Revised membership and updated contact information
8/2014	Greg Baker	2.2	Revised membership and updated contact information
10/2014	Mike Douglas	2.3	Revised contact information
5/2015	Mike Douglas Adam McGill	3.0	Annual review/update
8/2016	Mike Douglas	4.0	Annual review/update

© 2016 Equifax. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC.

CAT Team Contact List

Role	Primary	Alternate
CMT Member	**Susan Mauldin** susan.mauldin@equifax.com 678-795-7372 – work Redacted – mobile – home	**Doug Steelman** doug.steelman@equifax.com
CAT Leader	**Dodd Williams** Bryce.williams@equifax.com 770-740-4684 – work Redacted – mobile – home	**Matt Modica** matthew.modica@equifax.com 314-214-7273- work Redacted – mobile
Incident Manager	**Mike Douglas** michael.douglas@equifax.com 770-740-7313 – work Redacted – mobile – home	**Dodd Williams** Bryce.williams@equifax.com 770-740-4684 – work Redacted – mobile – home
Life Safety/Physical Security	**Matt Hyman** matthew.j.hyman@equifax.com 404-885-8442 – office Redacted – cell – home	**Sheree Franklin** Sheree.Franklin@equifax.com 404-885-8339- office Redacted – cell
Cyber Threat Center	**Doug Steelman**	**Francis (Frank) Finley** francis.finley@equifax.com 571-267-6450 – work Redacted – mobile
Investigations	**Greg Baker** greg.l.baker@equifax.com 678-795-7103 – office Redacted – cell – home	**Tony Alig** Mark.Alig@equifax.com 770-740-4710 – office Redacted – mobile
Security Engineering	**Diab Hitti**	**Andrew Gingher**
Corporate Communications	**Dianne Bernez** dianne.bernez@equifax.com 404-885-8325 - work Redacted – mobile – SMS	
Legal	**Troy Kubes**	**Julia Houston** julia.houston@equifax.com 404-885-8510 – work Redacted – mobile – home

© 2016 Equifax. All Rights Reserved

EQUIFAX, INC., "REGIONAL CRISIS MANAGEMENT PLAN"

EQUIFAX

Regional Crisis Management Plan

Southeast
Crisis Action Team Plan

May 2017

Version 2.0

The Southeast Regional CAT can be activated through the Equifax Notification System or via call tree. Activation should be initiated by CAT Leader or Alternate.	
Primary CAT Assembly Point	1505 Windward Concourse Alpharetta, GA 30005 Fusion Center Conference Room 1st Floor - Building 1
Secondary CAT Assembly Point	Virtual Conference Room
Conference Bridge Line	**BCP Crisis Management Bridge Line** **Bridge #:** Redacted **International Toll:** Redacted **Southeast Toll Free:** **Passcode:** **Hostcode:** Redacted

This Document is not an Emergency Response Plan.
In Case of Fires, Injuries, Threatening Situations, or Other Emergencies:

Get to a Safe Place and Call 911

(Outside US: Contact Local Emergency Services)

Serious incidents should be reported as a potential Equifax crisis:

- Fatalities, serious injuries, threatening situations, or natural disasters.
- Fires, explosions or other events causing damage to a facility.
- The risk or actual occurrence of confidential data corruption, loss, theft, or compromise.
- Any incident causing the evacuation or shelter in place of personnel.
- Facility closure due to severe weather or other regional emergencies.
- The risk or actual occurrence of significant operational disruption from any cause.

Incidents that might be an Equifax crisis should be reported by calling the Equifax Fusion Center Hotline:

+1 770.740.5555

Suspected information security incidents will be reported to the Cyber Threat Center (CTC) by phoning:
+1 678-795-7106 or 1-888-257-8799 or emailing:
security.incident@equifax.com.

Equifax's first priority is to protect the health and safety of people.

Once actions are underway to protect people, the action lists found in this Crisis Action Plan should be used to guide the overall response.

Table of Contents

Emergency Response

The number of trained emergency response staff at each Equifax locations varies by location depending of the number of personnel at the location and other factors. All sites have established Emergency Response Management Plans. Locations with sole occupancy have an established ***Emergency Response Teams*** and trained emergency responders. Locations without sole occupancy have assigned personnel, typically an office manager or most senior leader in the office, to be responsible for emergencies.

A list of locations with the level of emergency response capabilities is maintained by the Equifax Fusion Center. During a site emergency, the emergency response aspects of the incident will be managed according to the type of plan in place.

- If a crisis is declared in response to a site emergency, the site emergency response representative will:
- Implement the emergency response plan or general emergency guidelines for the site.
- Manage and direct all Equifax emergency response resources at the incident scene or related to the incident scene, including the CAT on-scene team.
- Designate an on-scene person to communicate with the CAT.
- Designate the on-scene Equifax spokesperson as appropriate (spokespersons to be approved in advance by Communications).
- Determine if external emergency responders should be called.

Emergency Response Team

The Emergency Response Team provides support to the Site Incident Commander, assess additional company needs for crisis response, and keep the Crisis Action Team (CAT) informed of events at the scene. The On-Scene Team Leader or Communications Member may act as a local company spokesperson in lieu of site management. Any CAT member may be designated to participate as a Response Team member. The Response Team may also include site personnel dedicated to corporate response activities at the time of the incident.

Once the emergency has stabilized and the health and safety of people has been secured, than the assessment of business operations and any additional response actions will be handed over to the Crisis Action Team.

External Emergency Response Command

If the emergency requires an external response, e.g., if 9-1-1 (or similar external emergency dispatchers in international locations) is called or a fire alarm is activated, then leadership of the emergency response is taken over by local (non-Equifax) emergency responders. In this case, the local officials will usually establish an Emergency Operations Center ("EOC") and designate a local Incident Commander. The local Incident Commander is typically the Fire Chief or Police Chief. In extreme situations, state or federal emergency responders may take over the local Incident Commander's role.

© 2016 Equifax. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC.

If an external response is active, the site emergency response representative will also:

- Unify command with the local Incident Commander, by using the Incident Command System[1] protocol followed by most federal, state and municipal agencies.
- Coordinate resources and response tactics with the local Incident Commander

[1] Most city, county and state response organizations in the US, use the Incident Command System ("ICS"), a standardized on-scene emergency management system, which includes an integrated organizational structure designed to reflect the complexity and demands of single or multiple incidents without being hindered by jurisdictional boundaries. (International locations may or may not have a similar system.) The ICS model uses a combination of facilities, equipment, personnel, procedures, and communications protocols operating within a common organizational structure. It is intended to aid in managing resources during emergencies and is applicable to both small and large incidents. The ICS plan provides a process for private sector representatives to assume various positions in the on-scene incident command post and the Emergency Operations / Joint Information Center for the lead responding agency.

© 2016 Equifax. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC.

Southeast Crisis Action Team Plan

During a Response, be sure to use the "Initial Actions – Response Level Activation"

Crisis Action Team Plan Purpose

The Southeast Crisis Action Team ("CAT") Plan defines the principles, roles and responsibilities for team members who respond in an expedient and orderly manner to unplanned events that impact the business. The goal is to minimize the impact of any event, resulting in an outage that could compromise service delivery of critical operations for Equifax. This team is known as the Southeast Regional CAT.

This plan is not intended to stand alone; it is used to support the ***Equifax Crisis Management Program*** (***"CMP"***) and the Equifax Crisis Management Team ("CMT"). All Southeast Regional CAT members must be familiar with the details of the *CMP*.

This plan provides a "Potential Considerations List" for Southeast CAT members, designed to ensure a consistent, collaborative response during a crisis by all active CATs.

The Southeast CAT is activated by the CAT Leader or the Incident Response Coordinator. It will be implemented in context of the ***CMP***. The responsibilities of the EFX CMT member are listed in ***Table A*** of the ***CMP***.

Crisis Management Principles

Scope: The Southeast CAT scope is typically limited to the Southeast management team response to an incident that has been declared a corporate incident or corporate crisis by the CMT; however, the Southeast CAT may also be activated by the organization for its own regional purposes, if appropriate.

Focus: The primary focus of the Southeast CAT is on the regional operational services, et al. and on issues that cut across organizations or departments. The Southeast CAT will also support or consult with other affected departments and offer specialized resources available at the regional or corporate level.

External Resources: The Southeast CAT may require additional resources beyond those within the company. In all cases of external resources, the resources will be considered part of the Southeast CAT and will operate under the direction of the Regional CAT Team.

Operational Guidance: The **Southeast** CAT will use the Potential Considerations List to manage the department response. Please note that all actions on the list may not be appropriate in every incident, nor are these the only actions required for a successful response. In all cases, judgment should be used to determine the correct actions.

© 2016 Equifax. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC.

Crisis - Definition

A crisis is an unplanned event related to Equifax's business that has the potential to:

- Present a significant threat to human health, safety or the environment.
- Cause a significant adverse effect on Equifax's reputation.
- Cause a significant disruption to Equifax's business.
- Create a perceived or actual violation of a regulatory or compliance standard.
- Cause a significant disruption or outage to Equifax's technology infrastructure.

Notwithstanding the definition above, a crisis is any event identified as such by the CAT Leader or designate.

Examples of potential Equifax crises may include:

- Operational issues such as office/data center emergencies.
- Significant outage of an Equifax system or application that may exceed the established Recovery Time Objective (RTO).
- Any situation that attracts the attention of the media and the public and could damage the reputation of Equifax.
- Natural disasters such as hurricanes, earthquakes, flooding
- Public health disasters, epidemics or pandemics.
- Financial crises, such as significant market-related situations, a major decline in earnings, or fraud.
- Informational crises, such as a loss of proprietary and confidential information, tampering with computer records, security incident or loss of IT infrastructure.
- Legal issues, such as the indictment or arrest of a senior executive.
- Regulatory issues, such as notices or inquiries from a regulatory or State Attorney General.
- Political/Civil unrest impacting business operations or personnel.
- Loss of the use of major offices /data centers for any other reason.
- Any information security incident involving PII, PCI, data compromise and/or exfiltration.

The Regional CAT is activated when the CAT Leader (or designate) decides an event meets or has the potential to meet the definition above. Further information on activation procedures is provided in **Activation Framework Overview**.

© 2016 Equifax. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC.
EFXCONG-SBC000000109

Contact List

Role	Primary Contact	Secondary Contact
CAT Leader	**Susan Mauldin** susan.mauldin@equifax.com **O:** +1 (770) 740-4500 **M:** **H:** Redacted	**Bryce Williams** dodd.williams@equifax.com **O:** +1 (770) 740-4684 **M:** **H:** Redacted
CM Coordinator	**Michael Douglas** michael.douglas@equifax.com **O:** +1 (770) 740-7313 **M:** **H:** Redacted	**Bryce Williams** dodd.williams@equifax.com **O:** +1 (770) 740-4684 **M:** **H:** Redacted
BCP	**Katalina Reynolds de Otegui** Katherine.Reynolds@equifax.com **O:** +1 (678) 231.0812 **M:** **H:** Redacted	**Chris Kennedy (ATL)** Chris.Kennedy@equifax.com **O:** +1 (770) 740-7918 **M:** **H:** Redacted
Security	**Greg Baker** greg.l.baker@equifax.com **O:** +1 (770) 740-4499 **M:** **H:** Redacted	**Matthew Hyman** matthew.j.hyman@equifax.com **O:** +1 (678) 591-5534 **M:** **H:** Redacted
IT	**Michael Ligetti** michael.ligetti@equifax.com **O:** +1 (770) 7406556 **M:** **H:** Redacted	**Jason McNair** Jason.McNair@equifax.com **O:** +1 (770) 740-5707 **M:** **H:** Redacted
Real Estate	**Karen Dick** Karen.Dick@equifax.com **O:** +1 (770) 740-4064 **M:** **H:** Redacted	**Shelton Anderson** shelton.anderson@equifax.com **O:** +1 (770) 740-5848 x5848 **M:** **H:** Redacted
HR	**Shari Lotz** Shari.Lotz@equifax.com **O:** +1 (770) 2862736 **M:** **H:** Redacted	**David Roth** David.Roth@equifax.com **O:** +1 (770) 296-4950 **M:** **H:** Redacted
Communications	**Ines Gutzmer** ines.gutzmer@equifax.com **O:** +1 (404) 8858555 **M:** **H:** Redacted	**Susan Chana** susan.chana@equifax.com **O:** +1 (404) 885-8907 **M:** **H:** Redacted
Legal	**Jennifer Burns** Jennifer.Burns@equifax.com **O:** +1 (404) 885-8095 **M:** Redacted	**Troy Kubes** Troy.Kubes@equifax.com **O:** +1 (770) 3290487 **M:** Redacted

© 2016 Equifax. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC.

	H: Redacted	H: Redacted
Finance	**Nuala King** Nuala.King@equifax.com O: +1 (404) 885-8440 M: H: Redacted	**Trevor Burns** Trevor.Burns@equifax.com O: +1 (470) 373-1108 M: H: Redacted
Global Operations	**Scott Vogt** Scott.Vogt@equifax.com O: +1 (770) 740-4825 M: H: Redacted	**David Meaden** David.Meaden@equifax.com O: +1 (678) 218-2914 M: H: Redacted
Marketing	**Aparna Shah** Aparna.Shah@equifax.com O: +1 (404) 885-8103 M: H: Redacted	**Anirudha Pradhan** anir.pradhan@equifax.com O: +1 (314) 610-8692 M: H: Redacted
Corporate Development	**Leigh Ann Groome** Leigh.Ann.Groome@equifax.com O: +1 (404) 885-8496 M: H: Redacted	**Kelly Heape** Kelly.Heape@equifax.com O: +1 (404) 885-8123 M: H: Redacted
PSOL	**Assad Lazarus** Assad.Lazarus@equifax.com O: +1 (678) 795-7248 M: H: Redacted	**Mike Teefey** mike.teefey@equifax.com O: +1 (678) 795-7304 M: H: Redacted
USIS	**Craig Crabtree** Craig.Crabtree@equifax.com O: +1 (770) 740-4602 M: H: Redacted	**Julie Anderson** Julie.Anderson@equifax.com O: +1 (770) 841-2391 M: H: Redacted
International CAT Liason	**Shahid Charania** Shahid.Charania@equifax.com O: +1 (404) 885-8611 M: H: Redacted	**Mark Rohrwasser** mark.rohrwasser@equifax.com O: +1 (470) 298-1065 M: H: Redacted
Auburn, AL Leader	**Brandon Holcomb** brandon.holcomb@equifax.com O: +1 (404) 2106682 M: H: Redacted	**Emily Traylor** emily.traylor@equifax.com O: +1 (404) 394-6236 M: H: Redacted
Charleston, SC Leader	**Gerard Baldwin** gerry.baldwin@equifax.com O: +1 (843) 375-4307 M: H: Redacted	**Brad Renfroe** brad.renfroe@equifax.com O: +1 (843) 375-4314 M: H: Redacted

© 2016 Equifax. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC.

Greenville, SC Leader	**Douglas Rawls** Doug.Rawls@equifax.com **O:** +1 (314) 214-7190 **M:** **H:** Redacted	**Amy Rush** Amy.Rush@equifax.com **O:** +1 (864) 350-2591 **M:** **H:** Redacted
Wilimington, NC Leader	**Shawn Nasseri** nobody.otho@iqn.com **O:** **M:** **H:**	**Ellen Stanko** Ellen.Stanko@equifax.com **O:** +1 (314) 214-7108 **M:** **H:** Redacted
Risk Management	**Idetta Curtis** idetta.curtis@equifax.com **O:** +1 (404) 885-8559 **M:** **H:** Redacted	**Rachel Olson** rachel.olson@equifax.com **O:** +1 (404) 885-8976 **M:** **H:** Redacted

CAT Assembly Sites

Southeast	Primary	1505 Windward Concourse Alpharetta, GA 30005 Fusion Center Conference Room 1st Floor - Building 1
	Secondary	Virtual Conference Room

© 2016 Equifax. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC.

Activation Framework Overview

Phase 1: Assess the Situation & Assemble the Team. Event reported to Incident Manager for activation assessment.

The Incident Managers will assess the threat, seek guidance from other leadership if needed (Regional GM, BU Heads), and then determine the level of CAT activation required. The Incident Managers are notified via the Fusion Center and/or a member of the Equifax Management Team and includes:

- Michael Douglas
- Dodd "Bryce" Williams

Before activating the Regional CAT, the Incident Manager, in discussions with the local site leader, will decide on an appropriate activation level based on the specific circumstances of the incident. The level can escalate as necessary to acquire resources for crisis response. All serious incidents must be reported to the CAT Leader or designee immediately. If there is any doubt about the activation level, the Regional CAT should be, at a minimum, activated at the **Notify Only Level**.

Activation Level Decision: No Action, Notify Only, Stand-by, Respond.

Notify Only Level
The CAT is notified when an incident is not an obvious Equifax crisis initially, but which warrants monitoring or would be of interest to members of the CAT. At this level, **CAT Members DO NOT respond or assemble**. Members are typically informed of the event during normal hours, typically via e-mail, and the Incident Assessment Coordinator becomes responsible for tracking incident status.

Stand-by Level
The Regional CAT may be put on "Stand-by" when an incident has the potential to become a Equifax crisis but CAT assembly is not yet appropriate. During this stage, CAT members will be notified of the incident and placed on notice that the team may be activated in the future. CAT members should then be making the appropriate arrangements to ensure the CAT is staffed for their function. **CAT Members DO NOT assemble at the Stand-by level.**

Respond Level
The Regional CAT will be activated when there is a high potential for a Equifax crisis to occur. The activation can occur immediately upon initial notification or as an event escalates from a lower activation level. All CAT members will be notified of the incident and be asked to attend an initial briefing. Declaring "Respond-level" activation immediately invokes the Regional Crisis Action Plan. Regional CAT activation will typically use the Mass Notification System.

© 2016 Equifax. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC.

Communicate to the Regional CAT if needed.

In all situations when the Incident Response Coordinator has determined the incident warrants CAT activation at any level, CAT members will be notified as described above. If the CAT is assembled, the Mass Notification System will be activated and simultaneous communication to all CAT members and alternate members will occur. All documented contact points will be involved (Office Phone, Cell Phone, Home Phone, E-mail, etc.). In most cases, a conference line will be provided as part of the activation process.

Only proceed to Phase 2 if a RESPOND level activation is declared.

Phase 2: Prepare to conduct the Initial Briefing

- Collect information.
- Prepare agenda (next page).

Phase 3: Conduct the Initial Briefing (For all CMT members and alternates– usually a call)

- Brief team.
- Discuss actions that are required immediately.
- Determine what cross-functional coordination is required.
- Specify next meeting time/location.
- Discuss CAT activation.
- Activate CATs and review situation. Get CAT input.

Phase 4 Conduct second meeting (CMT assembles)

- Use pre-determined agenda (next page).
- Status report from affected site/business.
- Status reports from each function (include information from CAT briefings).

Phase 5 Continue Response Activities

- Conduct routine meetings using Brief, Discuss, Action model.
- Continue management of crisis.

Phase 6 Conclude the crisis response (Recovery)

- Stand down CAT – move into recovery stage.
- Assign responsibility for on-going management efforts.
- Charter incident investigation team as necessary.
- Conduct After Action Review.

© 2016 Equifax. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC.

Initial Actions – Respond Level Activation

Review Guiding Principles and Priorities:

1. Place the highest priority on Life Safety – the welfare of all people including personnel, clients, visitors, emergency responders and community members.
2. Protect our assets and preserve our ability to operate and supply our clients.
3. Maintain a strong Equifax reputation through ethically and socially aware behaviors that ultimately preserve shareholder value.

AFTER Declaring a Activation

Initial Notification

- Receive briefing from Incident Response Coordinator.
- Confirm decision to activate CAT.
- Confirm plan for initial CAT briefing.
  - Time, location, call-in numbers, etc.
- Consider the need to inform the International Crisis Action Team or Corporate Crisis Management Team.
- Consider the need to inform any regulatory agencies.

Prepare for initial CAT briefing

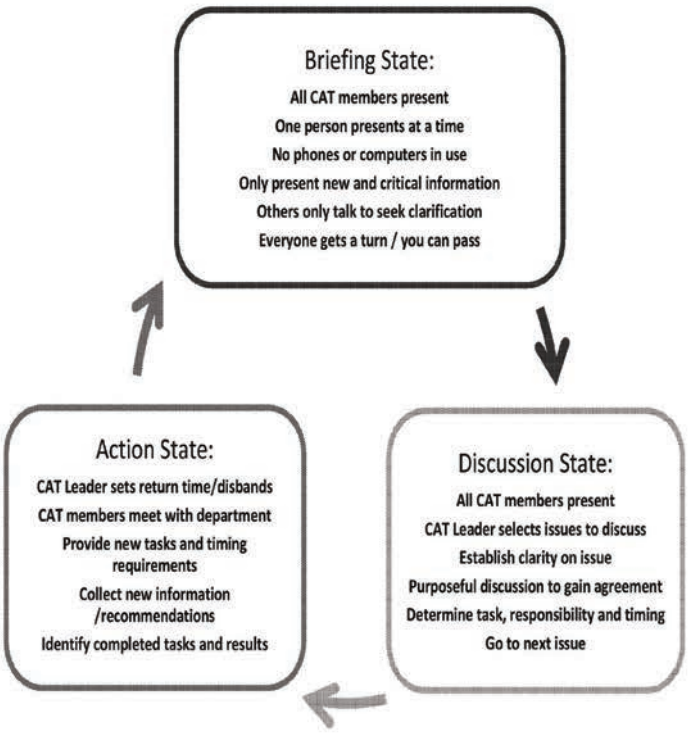
- Review the Initial CAT Briefing Agenda (below) to confirm responsibilities.
- If possible, obtain an updated status of the incident.
- Consider the timing for the first full CAT meeting.

Agenda Topic	Desired Outcomes
Purpose of the call	Brief the Team. Direct Admin Support member to document all facts and decisions.
Identify all callers	Document all callers and ensure all CAT roles are represented.
Situation Description	Provide the current details of the situation to the CAT.
Support	Identify support requested by the site or business. Discuss the potential additional support the CAT may be required to provide.
Team Selection	Identify the team members (name and role) that will continue to support this event.
Communications	Determine what communications have been made and what communications are still required. Assign responsibilities.
Logistics	Announce next meeting time and location (meeting room and telephone numbers).
Adjourn meeting	Final concerns issues. Direct CAT members to assemble, brief and provide direction to his or her support team.

© 2016 Equifax. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC.

CAT Meeting Process



© 2016 Equifax. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC.

CAT Team Roles and Responsibilities

The primary roles and responsibilities of the Southeast CAT are listed below:

- Acts as primary counsel to the CAT on all aspects of the operation in his or her area of responsibility including:
  - Local governmental requirements and laws.
  - Cultural expectations and norms.
  - Local conditions such as community reactions, media coverage, physical conditions, etc.
  - Travel logistics.
  - Security conditions.
- Provides on-site or regional presence to assist in managing the event, as directed by the Incident Response Coordinator.
- The CAT Leader may act as an Equifax spokesperson, if directed by Corporate Communications Leadership.
- Oversees the entire local response process
- Activates and may provide guidance to the region's ***Business Continuity Plans*** as directed by the Incident Response Coordinator.

© 2016 Equifax. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC.

Southeast CAT – Potential Considerations List

Please note that all actions in the list may not be appropriate in every incident, nor are these the only actions required for a successful response. In all cases, judgment should be used to determine the correct actions.

Initial Actions and Assigning Resources (CAT Leader)

[] 1. Advise senior management of incident and reaffirm responsibilities. Review roles of Southeast Regional management and staff.

[] 2. Activate the Southeast Regional CAT and confirm meeting location.

[] 3. Review the need for outside suppliers. If needed, employ outside suppliers and have them operate under the direction of the Southeast Regional CAT.

[] 4. Assign a resource to account for all department employees, contractors and guests and report any missing, injured or unaccounted people to the assigned HR resource.

[] 5. Assign a resource to maintain information flow among the CMT, all other CATs, affected departments, and outside suppliers.

[] 6. Establish and communicate to the Southeast Regional CAT a method to capture action log and retain notes for post incident review.

[] 7. Activate additional staff as needed and assign tasks.

Southeast CAT Considerations

[] 1. Identify key products and partners (channel, and third party) that may be affected, and provide list to Business Units.

[] 2. Establish a daily product & services availability review schedule together with Global Operations.

[] 3. Work with Corporate Communications, Global Operations, Legal and Finance CATs to establish priorities under reflection of contractual obligations and obtain a plan for product availability.

[] 4. Establish a recovery schedule that is regularly updated and reviewed as a basis for ongoing communications with clients.

[] 5. Work with Legal CAT contact to determine impact of Service Level Agreements (SLAs)

[] 6. Recover the business as defined by the Business Continuity Priority Plan.

© 2016 Equifax. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC.
EFXCONG-SBC000000118

Security and Safety Considerations

[] 1. Brief Site security personnel and reception if appropriate.

[] 2. Assist HR to account for all people including staff, contractors and visitors. Each department will be responsible for their own staff and report findings to HR. HR will need information from Security and Facilities to aid in the search. Some data that they may need includes:

- Security badge data
- Visitors lists from front desk
- Hospital transport information as known

[] 3. Prepare and submit a security plan for the CAT Command Center and other critical facilities to the CAT leader.

[] 4. Initiate enhanced security procedures at all sites. Access control and security procedures elevated throughout the corporation as necessary.

[] 5. Receive and distribute to security personnel official company statement(s) from Communications CAT contact.

[] 6. Determine if CAT relocation is needed.

[] 7. Provide Security liaison to Municipal Authorities and liaisons to Fire/Police Incident Command Post as needed at the Emergency Operations Center. Work with Police for site and criminal issues (in conjunction with Legal). Be prepared to supply video, floor plans and other building information as appropriate.

[] 8. Contact outside service providers (Guard service, private investigators, law enforcement specialists, etc.) to alert them to the emergency and the potential need for assistance. Evaluate the provider(s) ability to quickly mobilize adequate resources upon request.

[] 9. Review and approve requests for additional security resources for Canadian office locations. This would include alerting security resources (Guard service, private investigators, Law enforcement specialists, etc.) of the emergency and potential need for assistance. Evaluate the provider(s) ability to quickly mobilize adequate resources upon request.

[] 10. Recommend that all other CATs provide a list of the authorized/restricted employees and contractors for the alternate worksite. Provide copy of list to Security for relocation efforts.

[] 11. Provide security advice and consultation for personnel traveling to the affected site.

[] 12. Provide executive protection for all potential threats to personnel.

[] 13. Continuously evaluate and mitigate threats, including threats to affected site and other company facilities.

[] 14. Provide frequent status updates to the CAT teams members.

[] 15. Monitor network security to prevent unauthorized access by former employees, media, etc.

© 2016 Equifax. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC.

[] 16. Contact security engineering for any additional resources and/or assistance.

[] 17. Provide notification and potential activation of the ***Security Incident Response Team***

[] 18. Oversee the authorization and implementation of the ***Security Business Continuity Plan***.

Real Estate Considerations

[] 1. Assess the situation and with the Security & Safety team, determine the best and safest location for the CAT to assemble.

- Is a conference call the only initial option?
- If a physical location, communicate the appropriate rooms for each team.
- Make sure selected rooms are safe and then set up the needed equipment and technology.
- Establish catering schedule to feed teams.

[] 2. Establish communications with facilities staff at affected sites.

- Assess basic services and if support is needed.
- Review the current situation status and recommend initial actions to the CMT and/or Southeast Regional CAT.

[] 3. Manage damage assessment activities.

[] 4. Identify potential new and/or temporary space alternatives if primary workspace is damaged.

[] 5. Obtain a list of prioritized business processes to relocate from the CAT. Ensure that the facilities relocation team receives direction on teams to be relocated.

[] 6. Work with authorities to determine if any facility closures are needed. If needed, arrange transportation for employees.

[] 7. Contact Security & Safety team to ensure appropriate security has been established for business operation groups at alternate site.

[] 8. Discuss the current situation, status and restoration activities with the facilities restoration team and report findings to the CAT.

[] 9. Set up a family meeting area, if CAT approves the need for one.

[] 10. Assess the effects of the incident on mail and courier operations.

- Determine a new location for deliveries if needed.
- Advise delivery services of the new location.
- Set up a procedure to get mail to the addressees from the new location.

[] 11. Include IT review for any production changes prior to deployment.

[] 12. Approve and authorize the implementation of the ***Real Estate Business Continuity Plans***.

© 2016 Equifax. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC.
EFXCONG-SBC000000120

Communication Considerations

Society/Media Aspects:

[] 1. Perform initial information gathering:

- What is the crisis?
- What are the immediate effects including human and business?
- Is there more to come?
- What is the worst case?
- What are the likely timelines?
- Has the incident been contained?
- What is being said on social media?

[] 2. Review staffing and the need for outside consultants.

- Determine need for and call in additional Communications support staff.
- If needed, employ outside consultants (i.e. PR Firm) and have them operate under the direction of the Communications team.

[] 3. Assign a person to maintain information flow between the CMT and all other impacted Regional CATs.

[] 4. Assign a person to manage information flow to the media and handle media calls.

[] 5. Assign staff to develop the Core Press Statement and talking points for business unit or company spokespersons.

[] 6. In conjunction with Security, determine if it would be appropriate to assign a Communications Liaison to the responding officials' Emergency Operations Center.

[] 7. Assess crisis effects to determine if the ***Communications Business Continuity Plan*** needs to be activated. If so, oversee determine timing, priorities and assign resources as appropriate.

[] 8. If needed, activate a Crisis Communications Center.

[] 9. As needed and directed by the CMT and/or the Regional CAT, dispatch and support On-Scene Team, including Communications Coordinator if appropriate.

[] 10. Identify and prioritize stakeholders; develop notification plan as appropriate. Consider key potential audiences groups:

1. Employees (US & International)
2. Customers (B2B and B2C)
3. Board of Directors
4. Media
5. Investors (Financial Community and International Partners)

© 2016 Equifax. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC.

6. Third-Party Stakeholders
7. Competitors
8. Government Officials
9. Regulatory Agencies
10. Advocacy Groups
11. Industry Associations
12. General Public

[] 11. Develop a Communications worst-case scenario including the potential for reputation damage for each stakeholder group. Determine whether to utilize PR firm for this step.

[] 12. Begin developing a media strategy based on CMT recommendations:

- Is media already on-site or at designated location?
- Media briefing location required?
- Recommend news briefings if appropriate.
- Reactive or proactive approach?

[] 13. Identify company spokesperson(s) and provide briefing support and guidance.

- Produce media alerts to advise media on time and location for Press Briefings.
- Prepare talking points for questions that are likely to be asked by the media.
- Review talking points with spokesperson prior to briefings.

[] 14. Identify an onsite spokesperson and provide with a Core Press Statement and follow-up news media briefing statements:

- Confirm/identify internal approval process for news media statements.
- Develop a media schedule for Press Briefings and releases.
- Produce media alerts to advise media on time and location for Press Briefings.
- Prepare talking points for questions that are likely to be asked by the media.
- Review talking points with spokesperson prior to briefings.

[] 15. Define all the specific media materials that need to be prepared for each audience.

[] 16. Expedite approval process for releasing information to the media and other audiences.

- Contact the list of defined contributors for crisis communication process
- Follow the approval process as defined in the Crisis Communications Plan
- Receive sign-off from those on the defined Approval list
- Release information as defined by the approved distribution channels in the Crisis Communications Plan.

[] 17. Assign resources to track social media and create timely response.

© 2016 Equifax. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC.

[] 18. Consider the need to activate translation services.

[] 19. Include IT review for any production changes prior to deployment.

[] 20. Monitor all media, including real-time monitoring of broadcast, social media and online. Implement a print, broadcast and online clipping service. Forward a copy of all collected coverage to the Legal team.

- Respond as needed to misinformation
- Establish a summary process for reporting media information to CMT

[] 21. Establish contact with Communications executives/staff in affected locations.

- Notify and coordinate with appropriate departmental personnel
- Offer communications resources from the Communications CAT (where there is a unique expertise as listed in Section C)
- Verify that Security is controlling the media at the affected site and deliver message that no video or cameras are permitted on Equifax property

Employee Aspects:

[] 22. Coordinate with HR to prepare and execute a communication plan for employees.

- If appropriate to situation, remind employees to notify their families that they are safe to reduce number of families calling in.
- Identify specific employee groups that need information.
- Communicate phone number for employees to use to get updated information.
- Identify information vehicles and craft appropriate message(s) to communicate to employees.

[] 23. Coordinate with HR to set up an employee hot line(s) for employees to call and receive information. Possible existing call centers and resource include:

- SendWordNow Notification System – (http://www.sendwordnow.net)

Customer Aspects:

[] 24. Assess effects on customers and determine necessary communications.

[] 25. Obtain and have available a list of all "call centers."

[] 26. Work with Bus and Global Operations to identify appropriate toll free numbers to use for customer response to the crisis, confirm numbers are staffed and publish numbers via appropriate customer communication channels.

[] 27. Create, distribute and update messages to be used by staff at all call centers as necessary

© 2016 Equifax. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC.

[] 28. Work with Bus and Global Operations resources to provide call center staff instructions about referring media calls.

[] 29. Activate and populate pertinent information on the internet.

[] 30. Consider the need to secure translation services at call center locations.

[] 31. Consider the need to implement probing surveys to further detail customer reaction to the crisis.

[] 32. Monitor and report call center and social media consumer feedback to the Communications CMT Member.

Human Resource Considerations

Payroll Process Function and Support

[] 1. Determine if there will be an impact to payroll and coordinate contingency planning.

- Compensation decisions for facility closure/delayed opening
- Approval process for over-time coverage
- Time-sheet approval process for employees and/or contractors

[] 2. Work with Finance to contact payroll vendor or service and provide decision on how to manage payroll cycle.

- Workday is payroll system of record for US locations.
- Will payroll file be delayed or sent outside of normal schedule?
- Can payroll vendor re-run last payroll file?
    - Run 40 hour week for US overtime eligible employees
    - Run 37.5 hours for Canada overtime eligible employees (may be autopaid).

*Payroll report will be run automatically through retro process once correct time is submitted.

HR Emergency Response (if applicable)

[] 3. Prepare a spreadsheet on the health status of employees, contractors, vendors and visitors in coordination with the Incident Commander and/or local authorities/public officials.

- Names and location (hospital) of injured and brief status of condition if available.
- Names of anyone killed.
- Names of anyone missing or unaccounted for.
- List of evacuated employees, contractors etc.

© 2016 Equifax. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC.
EFXCONG-SBC000000124

[] 4. Obtain report from Security and Emergency Management and report to CMT regarding response details:

- Number and status of victims
- Victim transport – which hospitals?
- Law enforcement involvement
- Evacuation status (if applicable)
- Access to building and property
- Immediately identified damage

[] 5. Work with Security to unify operations with local medical officials at the incident scene.

- Determine if employees have been injured or sent to hospital, and if hospitalized, assign hospital watch personnel.
- Determine if employee fatalities have occurred. If so, provide support as appropriate to assist public officials involved in next-of-kin notification. Coordinate information with Communications team, Regional CAT and/or CMT.
- Contact the health insurance company to inform them of incident and hospitalization of employees.

[] 6. Obtain Security badge list and visitor lists as possible from Security.

[] 7. Communicate with external vendors to alert them of the incident and coordinate efforts accounting for contractors that may have been site at the time of the incident.

[] 8. As possible, establish/activate employee information hotline.

[] 9. Provide support and information as possible to authorities to conduct Next of Kin Notifications.

[] 10. Coordinate closely with EAP for family notifications and support.

[] 11. Work closely with Communications team to develop messaging for employees and families.

[] 12. Establish ongoing communication with family members of affected employees:

- Establish phone number for family members to call. Establish pre-recorded message if necessary based on call volume.
- Lead the process of contacting the families of those injured, as necessary; provide information on the nature of the injuries and the name, location and phone number of the hospital where the injured employees have been taken.
- Send an Equifax representative to the hospital to which employee(s) was transported. If possible, send one company representative for each seriously injured person.
- Determine if need for a family gathering area off-site for affected families. Work with Security and Facilities/Travel teams for arrangements.
- Staff the family gathering area with EAP personnel – determine the need for

© 2016 Equifax. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC.

counselors at the hospitals or other locations to provide support to families.

- Establish and maintain a log of families checking into gathering
- For ex-pat families in Southeast review medical coverage and assist as possible.
- For ex-pat families affected abroad determine special needs such as repatriation of remains, visa issues, evacuation, etc. (Consult ISOS as needed for international incidents.)

[] 13. Work with EAP to arrange for counselors to assist employees upon return to work.

Human Resources Business Support

[] 14. Establish and maintain communications with HR leadership in the affected BUs and with the affected location(s) if not a main campus facility.

- Review relevant HR issues/policies (benefit plan summaries, coverage, etc.) and be prepared to respond to related questions.
- Assess basic services and if support is needed.
- Offer affected departments(s) Human Resources expertise from the HR team (where there is a unique expertise as listed in Section C).

[] 15. Determine which critical HR activities are time-sensitive and respond accordingly.

[] 16. Access and verify the contact listing of company, affected department and outside personnel who are essential in the HR team's ability to respond to this event.

[] 17. Assess the staffing impacts of the incident, including:

- Make recommendations to CMT if shifts should be cancelled or reduced and what communications should be sent to the general employee population.
- Establish or interpret policy on compensation of workers not reporting because of the incident. Address pay issues and benefits related to employees who are told not to come to work because of facility damage, etc. for a few days or weeks.
- Address policy for keeping people on payroll if site is shut down for an extended period of time (weeks to months).
- Assess the impact of staffing changes on agreements for contract employees.
- Address special temporary staffing needs and use of contractors and/or consultants. Confirm the dispatch of and the estimated arrival times of additional staffing.

[] 18. Accelerate/facilitate processing the following:

- Medical services
- Health benefits
- Other benefits (401(k) loans, withdrawals, etc.)
- Leaves (FMLA, DI, etc.)
- Life insurance claims
- Workers compensation claims

[] 19. Engage HR Representatives in identifying and responding to employee issues at the department level.

© 2016 Equifax. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC.

[] 20. Ensure HR staffing capability at backup or redundant facility; assist affected department to acquire temporary staff if needed. Ensure staffing is available throughout the "Return to Normal" transition. This may require additional staff to occupy both the recovery location and the "home" location.

[] 21. Prepare rapid training planning for employees as necessary to address technology skill transfer.

[] 22. Develop an HR-based worst-case scenario.

[] 23. Monitor location of employees and assess threats related to the incident on global employee base.

[] 24. Assess the need for unique high-level, external HR contacts at the company level. (For example Ministry of Labor)

[] 25. Evaluate HR record systems and special record retrieval activities at the affected site.

[] 26. Implement manual records (hard copies) as needed.

[] 27. Include IT review for any production changes prior to deployment.

HR Communication Issues:

[] 28. Work with Communications resources to ensure language of internal and external releases is protective of HR policies.

[] 29. Communicate the HR perspective on the incident on a regular and timely basis to internal audiences, specifically the CMT and other CATs.

[] 30. Prepare, in coordination with Communication CAT, a Communication Plan for employees.

[] 31. Oversee the entire employee communications process for the company's response with a perspective of maintaining employee morale and confidence.

[] 32. Provide input to CMT on whether employees should report to work.

[] 33. In conjunction with Communications, communicate to employees if they should return to work or not. Also possibly communicate any pay/benefits decisions during the crisis.

[] 34. Communicate regularly to employees about the incident and set up a process for employees to obtain updates on the crisis situation and for company HR to receive information from employees regarding questions. Provide answers to employee questions as necessary.

[] 35. Activate an employee hot line(s) to answer employees' questions.

- Establish incoming and outgoing communication capability
- Make preparations for translation of messages into all required languages

[] 36. Coordinate providing employees' access to TV/cable news stations at sites.

[] 37. Establish communications with contractor/vendor companies that may have employees on site (in coordination with IS).

[] 38. Evaluate potential for HR issues to spread to other areas or locations not immediately affected by the crisis.

© 2016 Equifax. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC.

Technology Considerations

[] 1. Offer IT resources to affected departments, especially when there is a unique expertise listed in Section C.

[] 2. Provide IT resources to external parties on the scene. Note: all resource requests must be balanced between the business need and IT Recovery via the IT team.

[] 3. Assess crisis to determine if the IT Disaster Recovery Plan needs to be activated. If so, oversee implementation and liaise between IT recovery operations and the rest of the company.

[] 4. Determine an IT worst-case scenario including the potential for widespread data or voice failure, data loss, unauthorized access to proprietary information, etc. Determine the need to lock down data center and if needed have authorities sweep data center.

[] 5. Establish and communicate to IT team a method to capture action log and retain notes for post incident review.

[] 6. Work with IT Service Desk and review number and types of IT issues.

[] 7. Coordinate the needs of the CMT and CATs including the items listed below in a secure fashion. The IT CAT member will coordinate with the Equifax Disaster Recovery Team and will request technology requirements. Ensure the IT Disaster Recovery Team secures and makes available all needed technology including:

- Send an IT resource to CMT location to provide support.
- Additional phone sets in meeting rooms, in conjunction with facilities group.
- Computers for anyone involved in the response that needs one. Configure the computer for appropriate applications access and provide user identification and password information.
- Provide initial access training to those using supplied computers.

[] 8. Maintain communications with other Equifax sites regarding the status of their network and any technology related issues that may affect them. Gather information from impacted sites regarding key items:

- Data center options.
- Business and systems capabilities.
- Nightly processing support.
- SLA breaches.

[] 9. Work with IT executives as appropriate, to declare an "IT Disaster."

[] 10. Work with all organizations to assess the impact of the incident on "business-as-usual" call handling and staffing levels. If needed work with telecomm providers to reroute crisis calls to eliminate effects on other departments.

[] 11. Communicate the IT perspective on the incident on a regular and timely to internal audiences, specifically the CMT and other CATs.

© 2016 Equifax. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC.
EFXCONG-SBC000000128

[] 12. Determine need (or not) to control/limit communication channels (e-mail filters, limitation, phone redirects, etc.)

[] 13. Work with Communications team to develop any messages regarding IT issues ensure that Equifax's "One Voice" message to customer/customer-facing teams is consistent.

[] 14. Provide "initial assessment" to the IT CAT member of current capabilities of the infrastructure with information provided by the IT Disaster Recovery Team regarding:

- Overall effects on all systems.
- Technology outages (including estimated durations).
- Timing of new set up.
- Available systems.
- Potential locations for business resumption based on buildings that have working infrastructure.

[] 15. Identify business needs and then shift resources as possible based on insights from the IT Disaster Recovery Team. Once priorities are decided, ensure IT Disaster Recovery Team executed recovery against established priorities.

[] 16. Ensure IT Disaster Recovery Team monitors activity on company and site phone systems and take required action to keep telecomm systems operational.

[] 17. Ensure IT Disaster Recovery Team monitors security of networks to prevent unauthorized access by former employees, media, and others. Assess if destructive code has entered the system or threatening emails.

[] 18. Ensure IT Disaster Recovery Team fills requests from the CMT and CATs for collaboration tools, remote data and voice access, teleconferencing and video-conferencing capabilities and supports these tools.

[] 19. Prepare the systems for extra workdays (Sat., Sun.) if needed. Review resources for IT Help Desk and increase number of staff and resources as needed.

[] 20. Work with Facilities to monitor and confirm delivery and receiving process of new or relocated equipment. Installation will be provided by the IT Disaster Recovery Team.

[] 21. Notify CMT when alternate locations are operational and application and data restorations have been completed.

Global Operations Considerations

[] 1. Advise employees of the situation and coordinate the actions associated with the Global Operations BCP plan.

[] 2. Recommend to CMT the actions needed to continue critical company operation processes, agree on tasks and priorities.

[] 3. Establish contact with the key sales and Global Operations leader(s) at the affected site(s) and obtain initial conditions and support needs.

[] 4. Evaluate the situation to determine if the disruption will compromise the ability to conduct and support business, for what period and which areas of Global Operations would be impacted by the disruption.

© 2016 Equifax. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC.
EFXCONG-SBC000000129

[] 5. Evaluate the potential financial effects of the disruption and provide an assessment to the CMT. If needed, determine the requirements for prioritizing services.

[] 6. Assess potential for the incident to affect other Global Operations. Those Global Operations potentially affected have been given situational guidance, e.g., shut down or increase preparedness.

[] 7. Communicate with external service providers to ensure safe, orderly services exist as the locations can handle them.

[] 8. Work with third party suppliers to ensure cooperation if the crisis involves their employees or locations.

[] 9. Assess the customer service Global Operations and provide recommendations to the CMT if Global Operations have been affected. Oversee the timely recovery of customer service Global Operations.

[] 10. Ensure customer service representatives have accurate information about the incident and have a scripted response to customer questions created in conjunction with the Communications CMT Member.

Legal Considerations

[] 1. Determine key legal and compliance issues and assess availability of internal/external resources that are required.

[] 2. Advise all functional areas of potential legal and compliance issues and assure appropriate response.

[] 3. Oversee the entire information gathering and recording process for the company's response with an eye toward discovery-related issues and record-keeping requirements. Advise those involved in incident response as to what types of written communications to make and what records to keep.

[] 4. Work with the Communications team to develop appropriate messages, including advice on internal/external communications.

[] 5. Coordinate with Records Management about salvaging/protecting existing vital records.

[] 6. Offer Legal Department resources from the Legal team to affected operations (where there is a unique expertise as listed in Section C).

[] 7. Appoint legal counsel on-site, if needed.

[] 8. Monitor, via the Security team, actions of local law enforcement officials at the incident scene if applicable. Assess the potential criminal aspects of the incident, including:

- Whether the company, its officers or any other employees or contractors may have potential criminal liability for the incident or the results of the incident. If so, assess need for representation and obtain if warranted
- Determine if the incident is related to or as a result of criminal action on the part of someone not associated with Equifax. If so, ensure local cooperation with criminal investigation in conjunction with Security.

[] 9. Develop contact with local regulatory officials at the incident scene if applicable. Assess the regulatory aspects of the incident, including:

© 2016 Equifax. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC.

- Determine if the required regulatory agency reporting requirements have been met.
- Determine if regulatory inspections are planned, and if regulatory actions are possible, and assign Legal Department resources to assist and monitor the audits.

[] 10. Assess the potential legal & compliance risks at the incident scene and at other sites, with specific focus on:

- The protection of employees and property.
- The protection of evidence and forensic state of the incident scene.
- Assess potential liability issues including:
  - Potential human health, personal injury and wrongful death claims.
  - Potential property damage claims.
  - Potential regulatory fines and penalties.
  - Potential supplier, vendor or customer breach of contract.

[] 11. Assess the need for unique high-level, external Legal Department contacts at the company level. (For example, the U.S. Attorney or local District Attorney, Administrators of Federal Regulatory Agencies, heads of key Non-Government Organizations; equivalents in other countries or regions.)

Finance Considerations

[] 1. Establish communications with the Finance Department staff at the affected site.

[] 2. Offer financial resources from the Finance Department to affected site (where there is a unique expertise listed in Section C).

[] 3. Create an estimated budget for crisis response activities and present to the CMT.

[] 4. Assess effects of crisis on reporting requirements and take necessary action. (e.g. tax, insurance providers, investment community, SEC and other regulators)

[] 5. Notify external agencies of the crisis situations as appropriate.

[] 6. Secure hard copies of books and records for reference if technology is not available.

[] 7. Obtain spending authorization from the CMT.

[] 8. Notify external auditors, via the CMT Leader of the crisis situations as appropriate.

[] 9. Assess clearing and settlement operations status.

[] 10. Assess Accounts Payable and Accounts Receivable/Credit operations and provide situation report to CMT.

[] 11. Identify manual options to provide Accounts Payable and Accounts Receivable/Credit process.

[] 12. Assess status of payroll operations and recommend methods to pay employees if normal technology is not operational.

[] 13. Report the incident to appropriate insurers and establish claims as needed.

© 2016 Equifax. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC.

- [] 14. Prepare a report for the CMT detailing the applicable coverage, deductibles and coverage limits.
- [] 15. Establish special cost center to collect/accumulate losses related to the crisis.
- [] 16. Track response costs for insurance purposes.
- [] 17. Recommend actions to reduce additional losses.
- [] 18. Coordinate with insurance providers and adjustors that will come to the site. Schedule adjustor visits considering the safety of access to the affected site.
- [] 19. Review response budget determine if cash availability is adequate.
- [] 20. Determine cash positions and assess if any actions are needed to protect access to cash.
- [] 21. Reach out to banks as appropriate to notify them about any potential irregularities in banking procedures.
- [] 22. Collect costs related to the incident to provide documentation of the loss. Verify the documentation is categorized by loss type according to policies in force.
- [] 23. Implement the ***Finance Department Business Continuity Plan***.
- [] 24. Assess/modify internal controls for the crisis management program.

© 2016 Equifax. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC.
EFXCONG-SBC000000132

Marketing Considerations

[] 1. Identify key products and partners (channel, and third party) that may be affected, and provide list to Business Units.

[] 2. Establish a daily product & services availability review schedule together with Business Operations.

[] 3. Work with Corporate Communications, Global Operations, Legal and Finance CATs to establish priorities under reflection of contractual obligations and obtain a plan for product availability.

[] 4. Establish a recovery schedule that is regularly updated and reviewed as a basis for ongoing communications with clients.

[] 5. Work with Legal team to determine impact of Service Level Agreements (SLAs)

Business Unit / Sales Considerations

[] 1. Identify key products and partners (channel, and third party) that may be affected, and provide list to CAT members.

[] 2. Establish a daily product & services availability review schedule together with IT and Global Operations.

[] 3. Work with Corporate Communications, Global Operations, Legal and Finance teams to establish priorities under reflection of contractual obligations and obtain a plan for product availability.

[] 4. Establish a recovery schedule that is regularly updated and reviewed as a basis for ongoing communications with clients.

[] 5. Work with Legal team to determine impact of Service Level Agreements (SLAs)

[] 6. Notify the CAT of any risks associated with losing the transaction during any acquisition activity.

[] 7. Determine if M&A activity will need to be suspended until after the crisis

Deactivation and Post Incident Actions

[] 11. Coordinate and disseminate "Return to Normal" message to employees, vendors, contractors, and other stakeholders.

[] 12. Compile all documented activities in incident status report. Collect and retain all notes and logs created during the event for later post-incident review.

[] 13. Deactivate Southeast Regional CAT and all response vendors as appropriate.

[] 14. Participate in debriefing sessions as directed by the CMT.

© 2016 Equifax. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC.

Accounting for People Guidance

The Security and/or HR Team is responsible for compiling all data about the status of people during a crisis; however, each departmental area is responsible for reaching out to their department's line organization or other resources to help account for their staff.

1. **Once safely out of the area of danger, assign a resource to track department staff status information.** Ideally, this person should not be member of your CAT, but another person who does not have another emergency management or crisis management role.

2. **If assembled physically, write down the names of people you know to be safe and the ones you cannot account for (within vicinity).** If you have evacuated, this may be chaotic, but write down as many names as possible. Ask employees if they know anyone to have been injured as well as any staff members that they know were not in the area of the incident (such as on vacation, traveling, etc.)

3. **Through chain of command within department, ask managers call out to check on employees and send results to assigned resource.** Ask managers to track their information and provide a summary to you at a regular interval (daily, every 3 hours, etc.)

4. **For identified injured employees, notify the HR CAT contact immediately!** Try to get additional information as possible about the location of the victim. Always document the source of information. What hospital? Has the family been notified?

5. **As possible, account for any contractors and guests and send to the HR CAT contact.**

6. **Do not contact families or conduct Next-of-kin notifications.** The HR team will coordinate all family notifications. Remember that some of the information collected in the immediate aftermath of an incident may be incorrect. If you have home numbers and are attempting to reach out to employees, be prepared to talk to family members. Calmly inform them that an incident has occurred. Instruct them to call back or have their family member call back when they see them. Do not speculate. Do not provide incident details, but be polite and compassionate.

7. **Accounting for people takes time. Keep HR regularly updated on your efforts.**

Send all of your information to the HR Team. Within the first hour of the response, the HR Team will reach out to each department contact to provide a method to receive your information. If you do not hear from the HR Team, send your information to EFXpeoplewatch@equifax.com.

Keep the HR Team updated regularly on your efforts. Accounting for people takes time!

© 2016 Equifax. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC.

Revision History:

Complete history of updates is captured within the Crisis Management Plan History Log field

Appendix A: Business Continuity Contact List

Plan	Primary Business Owner
Atlanta - Legal	Mauldin, Susan
Atlanta - Corporate Development	Groome, Leigh
Atlanta - USIS	Gardner, Michael
Alpharetta - Global Operations GF Commercial	Waid, Scott
Atlanta - Finance SFO USIS and Operations	Brandberg, Douglas
Alpharetta - IT USIS	Arashanapalli, Harish
Northpark - Global Operations GBS	Weeks, Anthony
Alpharetta - Global Office Automation	Wagner, Gregory
Atlanta - Finance Controllership	King, Nuala
Alpharetta - Marketing	Cavalheiro, Adriano
Atlanta - Finance Tax	Elwood, John
Alpharetta - InterConnect PS	Myers, Wade
Alpharetta - USIS	Brandon, Dennis
Alpharetta - Global Security	Mauldin, Susan
Alpharetta - Global Operations and Contributor Services	Rosedale, Drew
Alpharetta - Global Solutions Delivery CDC	Deignan, Andrew
Alpharetta - Global Solutions Delivery CMS	Vogt, Scott
Atlanta - Finance Investor Relations	Dodge, Jeffrey
Alpharetta - IFS	Andrade, Carlos

© 2016 Equifax. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC.

Charleston - WS_eThority Sales BU	James, Mark
Alpharetta - Global Sourcing Office	Brown, Timothy
Greenville - WS_Operations	Rawls, Douglas
Alpharetta - Global Consumer Solutions	Friedrich, Robert
Alpharetta - Global Platform Services	Ligetti, Michael
Atlanta - Finance Audit	Blalock, Christopher
Atlanta - Marketing	Gutzmer, Maria Ines
Northpark - USIS	Morrison, Daniel
Northpark - Global Consumer Solutions	Lazarus, Assad
Atlanta - Finance Treasurer	Bonfield, Michael
UK - Global Operations	Rudd, Janice
Alpharetta - Core Software Engineering (CSE)	Reid, James
Alpharetta - Global Corporate Platforms	Bayer, Nathaniel
Atlanta - HR	Bause, Michael
Northpark - Global Operations	Weeks, Anthony
Northpark - Finance	Bambarger, Richard
Atlanta_Real Estate-Procurement	Briscoe, Philip

© 2016 Equifax. All Rights Reserved

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC.

EQUIFAX, INC., "SECURITY INCIDENT HANDLING POLICY AND PROCEDURES"

EQUIFAX®

Security Incident Handling Policy & Procedures

October 2014
Version 9.5

Based on NIST Special Publication 800-61, Computer Security Incident Handling Guide, this manual establishes procedures for handling Security Incidents that may compromise the availability, integrity and confidentiality of Equifax data and resources.

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC.

Document Change Management

Document Name	Equifax Security Incident Handling Procedures		
Type:	Policy & Procedures	Equifax Policy No.	
Policy Owner:	Adam Magill	Issued By:	Global Security
Approved By:	Adam Magill	Prepared By:	Nick Nedostup
Effective Date:	June 2007		
Last Reviewed Date:	October 2014	Next Review Date:	October 2015

VERSION CONTROL

Date	Name	Versio	Description of Changes
May 2006	Nick Nedostup	1	Production document created.
June 2008	N. Nedostup, D. Amster, S. Choffery	6	Updated to combine Technical, Data and Physical Security Plans into one unified Security Incident Response Plan.
February 2009	N. Nedostup, D. Amster, S. Choffery	7	Yearly Updates
February 2010	N. Nedostup, D. Amster, S. Choffery	8	Yearly Updates
February 2011	N. Nedostup, D. Amster, S. Choffery	9	Yearly Updates
October 2011	N. Nedostup, D. Amster, S. Choffery	9.1	Updated to reflect organizational/employee changes. Added Document Change Management Section.
November 2011	N. Nedostup	9.1	Updated Section 3.1 to include frequency of IR Contact List review & updates.
March 2012	Ray Strubinger	9.1.2	Updated Appendix F and created a separate document for the information. Verified web addresses. Minor corrections to wording and terminology.
October 2012	Ray Strubinger	9.3	Update to DDoS procedure
June 2014	Francis Finley	9.4	Update to correct grammar, formatting, clarify language, and organization restructuring.
October 2014	Francis Finley	9.5	Update to fix section on Forensics/Malware handling, include additional contacts, Archer ticketing information.
October 2014	Ted Mac Daibhidh, CD	9.5.1	Standardized formatting throughout document; corrected various errors; restructured lists to be easier to reference/read, resized figures to be more readable; changed heading font and colours to match official template document; corrected "single point lists"updated ToC.

Table of Contents[TOC \o "1-3" \h \z \u]

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000138

1. General Information

1.1 Purpose

This manual establishes procedures for handling Security Incidents (SI) that may compromise the availability, integrity and confidentiality of Equifax data and resources. The purpose of an incident handling policy is to:

- Document, authorize and establish repeatable and predictable incident handling management standards, disciplines and processes within the Equifax Global Security that are acceptable as best practices.
- Facilitate cooperation and information exchange among all Equifax personnel who are responsible for detecting, identifying, declaring and reporting security incidents.
- Comply with Equifax Security Policy, Federal and State laws, Payment Card Industry (PCI) requirements, and National Institute Standards and Technology (NIST) guidance.

1.2 Mission Statement

The purpose of the Equifax Global Security is to provide governance of security related system monitoring, create a global discipline of security event monitoring, at the same time consolidating monitoring services under a single umbrella of Global Security Services. It has been established to take proactive measures to protect the global Equifax environment, respond to all suspected and verified security incidents across the global Equifax environment, develop and publish response procedures, and disseminate documentation and best practice recommendations to Equifax employees.

The goals of the Incident Response team are to:

- Stop unauthorized access or disclosure of Confidential data.
- Maintain and/or restore business continuity.
- Limit immediate incident impact within the Equifax IT environment.
- Limit immediate incident impact to customers and business partners.
- Preserve evidence.
- Determine how the incident occurred.
- Determine who/what initiated the incident.
- Ensure existing policies and standards are followed and updated in order to prevent further attack.

1.3 Scope

This manual applies to all Equifax businesses, affiliates, programs, teams, organizations, appointees, employees, contractors and other entities responsible for Equifax systems and data. For incidents involving PCI data Equifax will appropriately engage the payment brands per their respective incident response procedures.

All related Equifax Global Security documents, including the Equifax Security Incident Response Procedures are to be reviewed and tested semi-annually to ensure information is accurate and all relevant participants are educated on the process. Incident Response contact lists are to be reviewed and updated quarterly to ensure contact information is current.

The Equifax Security Incident Response Procedures includes processes for handling Security Incidents involving Equifax. It resides between Equifax Network Operations (Infrastructure Impacting/Normal Outages) and Equifax Disaster Recovery/Business Continuity Planning (fires, power loss, explosions, earthquakes, hurricanes, and/or severe accidents, etc.).

Such incidents include loss of data confidentiality, disruption of data or system integrity, disruption or denial of availability and violation or imminent threat of violation of the Equifax Security Policy or standard security practices.

Examples of Security Incidents are as follows:

- **Denial of Service:**
  - An attacker sends specially crafted packets to a Web server, causing it to crash.
  - An attacker directs hundreds of external compromised workstations to send as many TCP/ICMP requests as possible to the organization's network.

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000139

- **Malicious Code:**
  - A worm uses open file shares to quickly infect several hundred workstations within an organization.
  - An attacker or employee writes and/or loads code on a system with intentions of malfeasance.
  - An organization receives a warning from an antivirus vendor that a new virus is spreading rapidly via e-mail throughout the Internet. The virus takes advantage of a vulnerability that is present in many of the organization's hosts. Based on previous antivirus incidents, the organization expects that the new virus will infect some of its hosts within the next three hours.
- **Unauthorized Access:**
  - An attacker runs an exploit tool to gain access to a server's password file.
  - A perpetrator obtains unauthorized administrator-level access to a system and then threatens the victim that the details of the break-in will be released to the press if the organization does not pay a designated sum of money.
  - An internal user maliciously accesses or alters consumer data.
  - An external user inappropriately accesses consumer data.
  - An external user maliciously reports false data.
- **Inappropriate Usage:**
  - A user provides illegal copies of software to others through peer-to-peer file sharing services.
  - An employee uses corporate data for personal gain.
  - A person threatens another person through e-mail.
- **Data Loss:** A user errantly or maliciously attempts to transfer confidential data outside of the Equifax network in an unapproved manner.

1.4 Organizational Structure

Equifax Global Security will institute an internal centralized Security Incident Response Team (SIRT) model. This model defines a dedicated SIRT centrally located, that has full responsibility for all incident reporting, analysis, and response. The Equifax Security Incident Response Team (E-SIRT) manager reports to the Chief Security and Compliance Officer (CSCO). All permanent E-SIRT resources are located within the Global Security team.

This model provides a centralized team that can collect information from a wide variety of Constituent sources and quickly synthesize and disseminate it across the enterprise. The E-SIRT responds to reports of abnormal activity or other incident reports. It can also participate in incident and vulnerability analyses, lend expertise in testing or assessing the security of the enterprise, and play a proactive role in promulgating computer security awareness and training throughout the organization, if appropriate to the organizational structure.

The SIRT has full authority to analyze activity and full or shared authority to respond to incident activity as it occurs. No enterprise-wide action can be taken or recommended without the approval of the E-SIRT manager and upper management (e.g. VP of Cyber Threat Center or Chief Security and Compliance Officer).

The team also has the authority to enforce recovery and mitigation strategies with the approval and consent of upper management. Divisional and functional unit managers are notified of any action to be taken in their areas, and are involved in the decision-making process to determine how to implement a response. The team has the authority to release enterprise-wide advisories and other documents, including best practices, response and recovery steps, and security updates.

The team can also be responsible for reviewing and analyzing all IPS or other network/system/application logs. The organization determines whether the E-SIRT will visit victim sites in the parent organization to enact response efforts or whether they will recommend responses to be carried out by the local system, security, and network administrators in each division.

1.5 Reporting a Suspected Incident

Suspected security incidents will be reported to the Cyber Threat Center (CTC) by phoning +1 678-795-7106 or 1-888-257-8799 or emailing [HYPERLINK "mailto:security.incident@equifax.com" \h]

Individuals will be included in the Incident Response process based on need to know principals and will be engaged as documented in the Incident Response Escalation Manual. Two distinct groups will function during the Incident Response process, one technical, and one managerial. The technical team will receive approval from the management team to take action and provide status updates on a regular basis.

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000140

1.6 Services Provided

The CTC is responsible for monitoring, consolidating and correlating data from all Equifax security monitoring systems. Under the disciplined model, the Cyber Threat Center will govern all security monitoring technologies under the CTC, providing the following services:

- Proactive monitoring of unauthorized access attempts, inappropriate usage, denial of service and other suspicious and malicious activity.
- Distribution of security advisories.
- Centralized reporting.
- Incident response and handling.
- Performing vulnerability assessments.
- Provide user awareness and training.
- Coordination of disparate threats within a single monitoring group providing intelligent response services for the global Equifax enterprise.

1.7 Roles and Responsibilities

Core Incident Response Team Members

- **Security Program Manager (CSCO):**
  - Has final authority on all decisions relating to the management/response to a major security incident.
  - Responsible for notifying appropriate parties of all security incidents that could become the focus of media or administration interest and provide regular updates based on the severity of the threat.
  - Authorizes the release of incident related information.
  - Serves as the contact point with the communications department.
  - Ensures that system owners/business managers participate in the High level security incident damage assessment process with regard to determination of the value/sensitivity of information and review/concurrence in the final damage report.
- **Incident Response Team Manager (VP Cyber Threat Center, VP Global Corporate Security & Safety):**
  - Establishes a SIRT with the necessary skills and knowledge to quickly respond to threats.
  - Coordinates incident handling management of all EFX declared security incidents with oversight authority to ensure that all reports and responses are prepared, appropriate personnel are involved, appropriate organizations are contacted and proper actions are taken to resolve the incident.
  - Responsible for ensuring incident handling is accomplished by:
    - Ensuring that incident response personnel are assigned, trained, and understand their responsibilities in the organization's incident handling process.
    - Monitoring, reviewing, approving and ensuring timely incident closure.
    - Documenting, establishing, and implementing internal tactical procedures for reporting and responding to incidents to initiate and/or request assistance in complying with this directive.
  - Notifying the Security Program Manager immediately after confirmation that a security Incident has occurred.
  - Requests approval from the Security Program Manager to return compromised systems/applications to operational status; ensure that compromised systems/applications remain off line and disconnected from the network until approval is received.
  - Approves/disapproves system/application/web page return to normal operation within 24 hours of formal request.
  - Responsible for notifying the Security Program Manager with information concerning all security incidents and providing regular updates based on the gravity of threat.
  - In cases of illegal/inappropriate activities, refer the case to Human Resources for administrative actions against employees/contractors.
  - Assures that this procedure is modified as necessary, disseminated and enforced on behalf of the CSCO.

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000141

- Serves as the Department Point of Contact (POC) for collecting and analyzing information on incidents.
- Maintains contact with internal/external parties and provide whatever assistance is needed to ensure that activities required to resolve a security incident are taken.
- Coordinates with external forensics teams to gather, collect, and preserve computer evidence.
- Coordinates with departments to make decisions regarding the Security Incident. Possible decisions include: shut down of system, blocking of external/internal activity, or containment actions, as necessary.
- Provides progress reports on all open incidents per SLA guidelines.
- Provides copies of the latest information on security products, breaches and alerts to the department leaders to increase their level of security awareness.
- Takes the appropriate containment actions to provide adequate security in the company environment; assume the ultimate responsibility for final resolution of all security incidents.

- **Incident Response Team Coordinator**
  - Maintains security incident response checklists.
  - Maintains knowledge of the incident response plan and ensure that it is followed accordingly during an incident.
  - Coordinates bridge calls as directed by the Incident Response Team Manager.
  - Ensures accurate notes and milestones are recorded during the incident.
  - Secure meeting rooms and all related equipment as deemed appropriate by the Incident Response Team Manager.
  - Ensures that incident handling actions taken are in accordance with established policies and procedures including incident close out.
  - Maintains a current telephone and e-mail listing of all business unit leaders and their backups.
  - Makes certain that system administrators rapidly implement the actions required to mitigate or correct any identified incident and perform interim/follow-up activities until the incident is officially closed; Deviations should be noted to Incident Response Team Managers.
  - Reviews all requests for compromised systems/applications to ensure systems have been adequately patched/updated with security control prior to resumption of normal operations. In addition, review with the CTC the results of system scans.
  - Coordinates with outsourced NOC's and SIRT's, when required.
  - Provides a consolidated report on all open security incidents with progress on resolutions.
  - Coordinates with external forensics teams to gather, collect, and preserve computer evidence.
  - Provides a consolidated report on all open security incidents with progress on resolutions.
  - Provides progress reports on all open incidents per SLA guidelines.
  - Provides copies of the latest information on security products, breaches and alerts to the department leaders to increase their level of security awareness.

NOTE: The investigating CTC Analyst shall function as the IR Coordinator until escalated; other "Core Roles" will be brought in as necessary for SEV-3 or higher incidents only.

- **Legal Specialist:**
  - Maintains knowledge regarding the various laws related to security and privacy.
  - Ensures the E-SIRT does not violate any laws while investigating incidents.
- **Global Sourcing Specialist:**
  - Maintains knowledge regarding outsourced partners involved in any security incident.
  - Liaises with outsourcing vendors as needed to remediate items for which they are responsible.

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000142

- **Public Relations Specialist:** Sole point of contact to the media for the organization when it releases any incident related information, as authorized by the Security Program Manager.
- **Human Resources Specialist:**
  - Ensures that the E-SIRT does not violate employees' rights during the investigation of incidents.
  - Ensures that appropriate disciplinary methods are used if an employee is found to be the source of the incident.
- **Computer Forensics Expert:** Ensures that the investigation is performed in a methodical manner, seeing that evidence is collected and stored properly.
- **EFX Cyber Threat Center:**
  - Serves as a single POC for notifications of potential or actual Cyber Security incidents, 24 hours a day, seven days per week.
  - Receives reports of suspected security incidents from the following sources:
    - Internal or external sources.
    - System engineers.
    - Company employees.
    - Other sources.
  - Correlates global monitoring data in an effort to strengthen the security posture of Equifax by utilizing global data to identify attacks that might seem disparate when viewed individually.
  - Provides technical assistance and guidance in support of case investigations.
  - In collaboration with department CIO's, ensures that compromised systems have been patched and scanned before incident closure and approval to return to the network or before removal of blocked IP addresses.
  - Provides EFX organization E-SIRT members with technical expertise that will enable them to remediate the issue and complete incident report documents.
  - Reviews IPS procedures including IPS reporting formats to ensure that they are meaningful to the recipients and initiate changes in the IPS reports and firewall configurations to reduce intrusions.
  - Assists in the population a current electronic database of all security incidents and events.
  - Reviews all intrusion reports as received from reports from monitoring systems.
  - Assigns an EFX ITN to each case.

Incident Specific Team Members

- **System Administrators:** Gathers and provide data regarding system configuration and security as requested by the E-SIRT in an expedited manner.
- **Communication Specialists:** Gathers and provide data regarding network configuration and compromised system location as requested by the E-SIRT in an expedited manner.
- **System Developers:** Gathers and provide data regarding the server, system or application and any modifications thereto, as requested by the E-SIRT in an expedited manner.
- **Database Administrators:**
  - Gathers and provide data regarding the database and any modifications thereto, as requested by the E-SIRT in an expedited manner.
  - Verifies whether changes have been made to the compromised system database structure or configuration.
  - Verifies whether database specific programs have been modified.
- **System Owners: Facilitates and manage expedited service delivery over System Administrators, Communications Specialists, System Developers & Database Administrators.**

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000143

1. E-SIRT Activation and Initiation Process

2.1 Overview

The incident response process has several phases, from initial preparation through post-incident analysis. The major phases of the incident response process are outlined and summarized below. It is imperative that each of the phases is followed in a consistent and precise manner to ensure a rapid and thorough investigation.

Event notifications may occur from various entities as summarized below. Once the E-SIRT team has been notified of a potential incident, information will be gathered and initial analysis and investigation will occur immediately to validate and define a severity of the issue. This process is outlined in the Detection, Analysis & Activation phase below.

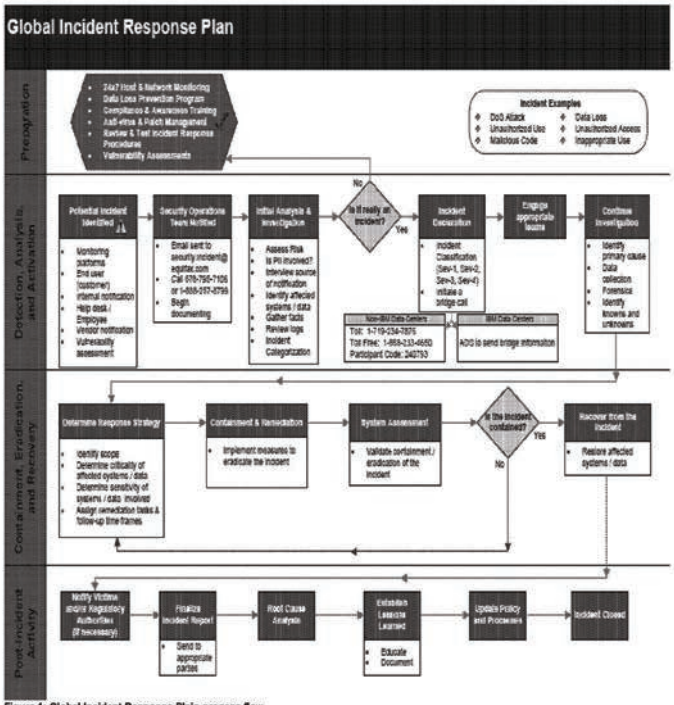


Figure 1: Global Incident Response Plain process flow.

Once the E-SIRT has validated and declared an incident, the Security Program Manager will be notified according to guidelines set forth by the Severity as defined in Appendix C. The Security Program Manager will then identify the appropriate Incident Response Manager, who will maintain ownership of the issue. This process is summarized in the following flow chart.

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000144

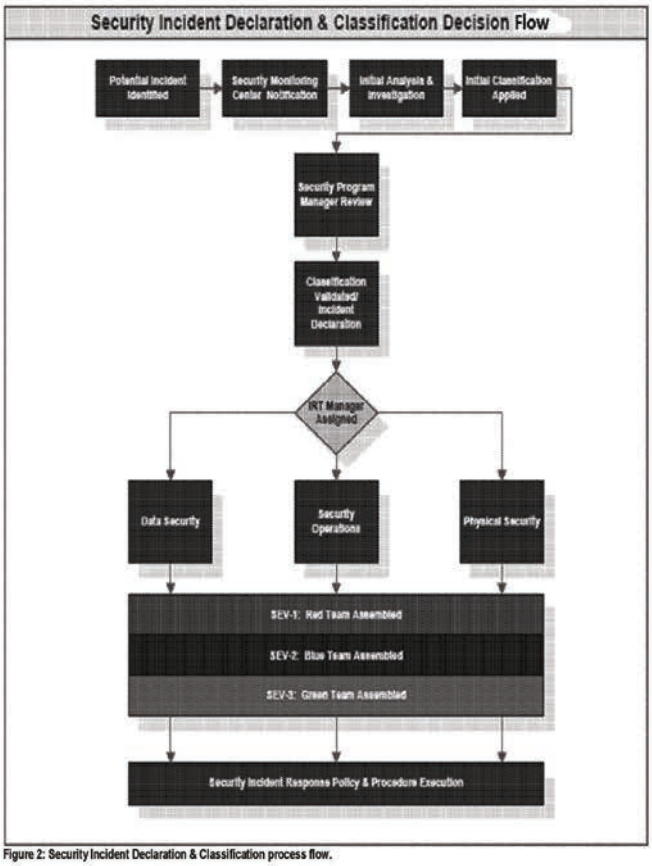


Figure 2: Security Incident Declaration & Classification process flow.

Technical bridges will be established for the E-SIRT to engage with appropriate IT and COE representatives while a Managerial Bridge will be established for updates from the Technical Team and approvals of Containment, Eradication and Recovery plans. Technical Bridges will be established according to procedures documented on the Cyber Threat Center Share Point site on a per-site basis.

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000145

2.2 Incident Response Management Bridge Procedure

2.2.1 Procedure Summary

This procedure summarizes the information which will be reviewed during Equifax Security Incident Response (E-SIRT) conference calls. The CTC Managers will maintain responsibility for scheduling and conducting the Management calls at the appropriate interval as defined in the Equifax Security Incident Response Manual (excerpt below).

	Severity Determination			
	SEV 4 (Informational)	**SEV 3 (Warning)**	**SEV 2 (Severe)**	**SEV 1 (Critical)**
Computer Incident Update Meetings	Weekly	Daily until contained. Weekly during business hours to close.	Every 4 hours until contained. Every other day during business hours to close.	Every 2 hours until contained. Daily during business hours to close.
Data Incident update meetings	N/A	As needed	Weekly until resolved.	Daily until resolved.

Table 1: Severity Determination matrix.

2.2.2 Procedure Details

Dial In Information

Toll Free: 1-866-628-8620

Toll: 1-719-387-5597

Participant Passcode: Redacted

Mandatory Participants (Or their representative):

Name:	Role/Responsibility:
Adam Magill	CTC Manager
Susan Mauldin	Chief Security & Compliance Officer
Susan Mauldin	Chief Privacy Officer
Diane Bernez/Tim Klein	Public Relations/Communications Specialist
Tim Brown	Global Sourcing Specialist
COE Representative	Provide details on business affected
Scott Hall	Global Disaster Recovery

Table 2: List of mandatory incident bridge participants.

Meeting Moderator Responsibilities:
An E-SIRT Manager will moderate the conference call.

1. Conduct and document roll call.
2. Remind all participants of confidentiality notice and that the information on the call is not to be shared with anyone outside of the call. Violations of this policy could result in disciplinary action, including termination. All requests for information pertaining to the incident should be directed to, and approved by, the Moderator for release. No information should be discussed with any customers/partners or media except as approved by the Public Relations Specialist.
3. Provide current status of the situation.
4. Document, assign and update action items and tracker.
5. Moderate open discussion.
6. Deliver meeting summary to Mandatory Participants following the meeting.

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000146

Participant Responsibilities:

1. Provide timely updates on status as requested by CTC Managers.
2. Provide guidance, advice and decisions related to issue on specific area of expertise.

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000147

3. Incident Handling Guidelines

3.1 Overview

Networks, information technology (IT) resources and Confidential Data are continually vulnerable to illegal/malicious activity or exploitation by internal and external sources. Incident Response (IR) handling is an important and required component of Equifax's Data Loss Prevention Program. Security related threats can exploit vulnerabilities in new or rapidly changing IT. The most common security threats are those that travel through and to networked systems. While it is impossible to eliminate all incidents, proactive incident prevention is a critical element of a mature incident management capability.

Preventative procedures such as user education, patch management, firewalls, intrusion prevention systems, risk and vulnerability assessments and mitigation can reduce incidents. Not all incidents can be prevented. A flexible and adaptable incident response capability is a necessary part of managing network security threats as damage to IT systems from a security incident can occur in a short period.

Standard reporting and uniform operating procedures permit Equifax to be better positioned for assessing risks, addressing vulnerabilities, reducing overall costs and meeting the security challenges of Equifax's information infrastructure. This document contains the procedures for handling reported and discovered security incidents.

3.2 Goals & Priorities

The goals of the Incident Response team are as follows. These priorities should be followed exactly as noted unless otherwise specified by the Security Program Manager or Incident Response Team Manager.

- Stop unauthorized disclosure of Confidential information;
- Limit immediate incident impact within the Equifax IT environment;
- Limit immediate incident impact to customers and business partners;
- Maintain or restore business continuity;
- Preserve evidence;
- Determine how the incident occurred;
- Determine who/what initiated the incident; and
- Ensure existing policies and standards are followed and updated in order to prevent further attack.

3.3 Incident Definition and Declaration

An incident is the act of violating an explicit or implied security policy. The types of activity that are widely recognized as being security incidents are violations categorized as, but are not limited to, attempts (either failed or successful) to gain unauthorized access to a system or EFX data, unwanted disruption or denial of service, the unauthorized use of a system for the processing or storage of data, or changes to system hardware, firmware or software characteristics without the owner's knowledge, instructions, and approval.

The level of consequence of an incident refers to the relative impact it has on an organization. The types of impact include: loss of data, the loss or theft of information, IT resources, revenue or confidence in an EFX company or mission area by the general public or customers; or a high level of damage that must be corrected prior to system restoration.

Within the Equifax Cyber Threat Center, security incidents shall be declared for the following reasons:

- Analysis of monitoring system reports that show signs of system compromises in the logs;
- Notification by an external entity of an EFX IP or e-mail addresses being the cause or victim of malicious or questionable activity;
- Alert, notification, or warning from other business partners, customers or departments that an EFX IP address(s) is the target or originator of malicious activity;
- Complaints by an Internet Service Provider (ISP) that detail specific, prohibited activities by an EFX host, IP address or e-mail address;
- Floods of viruses, worms and Trojan Horses for which anti-malicious code/anti-virus software is not available. In attacks where the attack vector and exploit code is similar/identical, one EFX incident number will be assigned for the entire process;
- Complaints from the public, or other employees that include specific examples or references of inappropriate or illegal use by EFX employees, cooperators, partners or contractors utilizing EFX IT; and
- A self-discovery by an EFX organization that meets the definition of an incident (i.e., virus discoveries, policy violations, criminal actions, etc.)

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000148

3.4 Incident Classification

Security incidents are declared when they are serious and considered major in nature. Declarations and classification will be based on an initial risk assessment of the situation including: number of affected systems; network impact; business services impact; sensitivity of information threatened or compromised, and the potential for harm to EFX (e.g. financial, service, sales, customer trust, or Equifax image impacts). Outlined below are criteria for security incidents (See [REF _Ref391199239 \h] for additional guidance):

SEV-1 (CRITICAL) incidents are events that involve compromise of Equifax systems or data, often involving multiple systems or data records or pose an immediate threat to facilities or employees. These incidents will be handled immediately and operate on a strict need-to-know distribution. Examples of CRITICAL incidents include:

- Recurring SEVERE incident;
- Threats posing eminent threat to facility or employees;
- Employee/contractor attempting to send Equifax Confidential data to an external personal email account/online storage or other external entity;
- Phishing attack against Equifax;
- Malicious data access and/or alteration by employee or contractor;
- Unauthorized access to data or systems, accidental or malicious;
- Hijacking of Equifax domains;
- Confirmed computer, network or application compromise;
- Disclosure, loss or corruption of critical data;
- Malicious files found on critical system;
- EFX website defacements or compromises;
- Successful DoS attacks by EFX systems or against EFX systems;
- Unauthorized use of a production system for processing or storing non-EFX or prohibited data or information; and
- Any violation of any local, state, federal or international law.

SEV-2 (SEVERE) level Security Incidents are potentially serious events involved a critical asset with moderate damage and should be handled within eight (8) hours after the event occurs or notification of the event is made to the EFX Global Cyber Threat Center. This would include inappropriate access to confidential data by an Equifax customer, vendor or other known third party.

- Recurring WARNING incident;
- Changes to system hardware, firmware or software without the system owner's authorization;
- Connection of unauthorized wireless access device to company network(s);
- A contractor or employee errantly or maliciously attempts to transfer Confidential data outside of the Equifax network in an unapproved manner;
- Abuse of resources impacting critical systems or services;
- Attempts to circumvent Equifax Security Controls;
- Misuse of company property, facilities or services including accepting payment or services to provide access to or use of EFX IT resources in excess of one's authority, such as forwarding spam, engaging in unofficial/unauthorized chat, non-EFX e-mail and instant messaging services; and
- Discovery of risk that could become CRITICAL

SEV-3 (WARNING) level Security Incidents involved non-critical assets and little damage. They should be handled within 24 hours after the event occurs or notification of the event is made to the EFX Global Cyber Threat Center.

- Recurring INFORMATIONAL incident;
- Employee/contractor who violates Equifax Data Classification policy through DLP violations inclusive of low volumes of data destined for a business;
- IPS reports that define activity as medium or unsuccessful system intrusion attempt;
- Unauthorized use of a system for processing or storing EFX data;
- Installation, use or sharing of unauthorized software;
- Unconfirmed computer virus/worms (depending on impact to department and if the infection is the result of a security policy violation);
- Undocumented or unapproved vulnerability scans;
- Isolated virus outbreaks; and
- Discovery of risk that could become SEVERE

SEV-4 (INFORMATIONAL) level Security Incidents are the least severe and should be investigated within two (2) working days after the event occurs. Informational incidents include:

- Lost employee/contractor asset (laptop, blackberry)
- Non-malicious employee incident (e.g. accessing own credit file)
- Individual PSOL incidents (e.g. ex-spouse)
- Suspected sharing of EFX accounts;
- Minor misuse of Company property, facilities and services;
- Unsuccessful scans/probes (internal & external); and
- Computer virus/worms (depending on impact to Company/Department);
- SPAM; and
- Discovery of risk that could become WARNING

Other types of incidents are categorized as adverse security events and shall not be declared security incidents unless there is a confirmed compromise of sensitive information, a threat to EFX data or subsequent escalation to a security Incident.

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000149

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000150

4. Incident Response Phases

4.1 Overview

Incident response methodologies typically emphasize preparation—not only establishing an incident response capability so that the organization is ready to respond to incidents, but also preventing incidents by ensuring that systems, networks, and applications are sufficiently secure. Such efforts must occur in many forms, including but not limited to the following:

- Collection of contact information for Core and Incident Specific Incident Response Team members, including pager, mobile, home, etc. numbers;
- Collection of contact information for Third Party Incident Response Team providers;
- Publication of incident reporting mechanisms;
- Execution of the Security Approval Process for Equifax Internet Systems;
- Collection and up keep of incident analysis hardware and software;
- Documentation of incident analysis resources (such as port lists, network diagrams, etc.);
- Incident response procedural documents for responding to the major incident categories; and
- Testing of the Equifax Security Incident Response Procedures

4.2 Detection and Analysis

Incidents can occur in countless ways, so it is impractical to develop comprehensive procedures with step-by-step instructions for handling every incident. The Equifax Cyber Threat Center and IRT therefore generally prepares to handle any type of incident and more specifically to handle common incident types, creating a discipline of security event monitoring, at the same time consolidating monitoring services under a single umbrella of Security Services.

Under the disciplined model, Security will govern all security monitoring technologies under the Cyber Threat Center (CTC), enhancing the capability to identify attacks that may include multiple sites and/or attack vectors. This consolidation into a single CTC discipline provides a stronger threat and risk management response by understanding the coordination of seemingly disparate threats within a single monitoring group to provide a more intelligent response for the global Equifax enterprise.

4.3 Containment, Eradication and Recovery

This Phase of Incident Response captures the —heat of the moment. This phase is entered when an incident has been detected and analyzed, and a Security Incident declared.

An essential part of containment is decision-making (e.g., shut down a system, disconnect it from a wired or wireless network, disconnect its modem cable, and disable certain functions). As such decisions are much easier to make if strategies and procedures for containing the incident are documented predetermined, Equifax priorities have been established in Section 3.2.

4.4 Post-Incident Activity

Conducting a lessons learned post mortem meeting addressing the following questions, and any others that arise is a critical part of the Incident Response process. Such meetings allow E-SIRT members to address that drive improvements in all previous Incident Response Phases. Questions such as the below should be addressed:

a. Exactly what happened, and at what times?

b. How well did staff and management perform in dealing with the incident? Were the documented procedures followed? Were they adequate?

c. What information was needed sooner?

d. Were any steps or actions taken that might have inhibited the recovery?

e. What would the staff and management do differently the next time a similar incident occurs?

f. What corrective actions can prevent similar incidents in the future?

g. What additional tools or resources are needed to detect, analyze, and mitigate future incidents?

Additionally, a follow-up report should be created for the management and extended team(s) as described below:

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000151

Incident Response Management

1. Prepare a report for Equifax Executive Management to include:
    a. Estimate of damage/impact;
    b. Action taken during the incident (not technical detail);
    c. Follow on efforts needed to eliminate or mitigate the vulnerability;
    d. Policies or procedures that require updating; and
    e. Efforts taken to minimize liabilities or negative exposure.
2. Provide the chronological log and any system audit logs requested by the Extended Team.
3. Document lessons learned and modify the Incident Response Plan accordingly.

Extended Team

Legal and Finance work with the local authorities as appropriate in the case that the incident; and HR and Corp. Security work with Equifax management to determine disciplinary action in the case that the incident was from an internal source

4.5 Incident Report Handling Guidelines

The Security Incident Response Team (E-SIRT) must ensure the controlled dissemination of all information pertaining to a security incident. To this end, the following guidelines should be followed when creating the Incident Report (IR) prior to communication and distribution of the report.

1. Label the report as "Confidential; refer to the Global Information Security Policy for more information on handling "Confidential" data. Section 4.4 contains special requirements.

2. The following disclaimer should be displayed on the first page of the IR (example cover page follows):

    ***"Security Disclaimer:** Access to the details of this report is only to be provided with authorization of the Chief Security & Compliance Officer (CSCO) following the Need to Know Security Principal. This document should not be disseminated without express permission of the CSCO. Failure to comply with this principal may result in disciplinary action up to and including termination."*

3. The following text should be hidden within the IR document, preferably within the header for consistency:-

    bR4yupequc7ab7ruCR4t3FEdR8PrUnuj

    To hide the text, change the colour of the font to white. A rule within the DLP application is set to block attachments containing this string and also to alert the VP Cyber Threat Center.

4. When stored electronically, the Incident Report should be encrypted with a company approved method of encryption. Refer to the Global Information Security Policy; section —7.13 Encryption Requirements for more details. The password for any such encrypted file should only be communicated between the Incident Response Team Manager and the Incident Response Team Coordinator. Any other password dissemination must be authorized by the Incident Response Team Manager.

5. CSCO approval of the distribution list must be granted prior to dissemination.

6. To prevent modification of the report, only distribute a version of the IR that has been created as a PDF. The PDF must also be encrypted in line with the requirements above.

7. When sending the IR via Lotus Notes set the delivery option to prevent copying of the email by performing the following:
    a. Select New Memo > Delivery Options; and
    b. Select the Prevent Copying checkbox, then OK.

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000152

5. Computer Incident Handling Checklists

5.1 Initial Incident Handling

The checklist in Table 3 provides the major steps to be performed in the initial handling of an incident. The items address only the detection and analysis of an incident; after that has been completed, incident handlers should use checklists that are geared toward a particular type of incident. Sections 5.2 through 5.7 contain handling checklists for each of the five incident categories. A generic checklist is provided in Table 3 for handling incidents that do not fit into any of the categories.

Note that the actual steps performed may vary based on the type of incident being handled and the nature of individual incidents. For example, if the handler knows exactly what has happened based on analysis of indications (Table3, Step 1.1), there may be no need to perform Steps 1.2 or 1.3 to further research the activity. The checklists provide guidance to handlers on the major steps that should be performed; they do not dictate the exact sequence of steps that should always be followed.

Initial Incident Handling Checklist		
	Action	Completed
	Detection and Analysis	
1.	Determine whether an incident has occurred	
1.1	Analyze the precursors and indications	
1.2	Look for correlating information	
1.3	Perform research (e.g., search engines, knowledge base)	
1.4	As soon as the handler believes an incident has occurred, begin documenting the investigation and gathering evidence	
2.	Classify the incident using the categories presented in Section 1.2 (e.g., denial of service, malicious code, unauthorized access, inappropriate usage, multiple component)	
3.	Follow the appropriate incident category checklist; if the incident does not fit into any of the categories, follow the generic checklist	

Table 3: Initial Incident Handling Checklist.

General Incident Handling Checklist		
	Action	Completed
	Detection and Analysis	
1.	Prioritize handling the incident based on the business impact	
1.1	Determine incident status, i.e. whether the incident activity is actively occurring or ceased	
1.2	Identify which resources have been affected and forecast which resources will be affected	
1.3	Estimate the current and potential technical effect of the incident	
1.4	Identify the primary cause or course of the incident	
2.	Report the incident to the appropriate internal personnel and external organizations	
	Containment, Eradication, and Recovery	
3.	Perform an initial containment of the incident	
3.1	Determine if incident recovery will require assistance from outside parties	
3.2	Validate containment of the incident	
4.	Identify and evaluate options to meet established goals	
5.	Acquire, preserve, secure, and document evidence	
6.	Eradicate the incident	
6.1	Identify and mitigate all vulnerabilities that were exploited	
6.2	Remove malicious code, inappropriate materials, and other components	
7.	Recover from the incident	
7.1	Return affected systems to an operationally ready state	
7.2	Confirm that the affected systems are functioning normally	
7.3	If necessary, implement additional monitoring to look for future related activity	
	Post-Incident Activity	
8.	Hold a lessons learned meeting	
9.	Create a follow-up report	

Table 4: General Incident Handling Checklist.

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000153

5.2 Denial of Service or Distributed Denial of Service (DoS or DDos)

A denial of service (DoS) is an action that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources such as central processing units (CPU), memory, bandwidth, and disk space. Examples of DoS attacks include:

- Using all available network bandwidth by generating unusually large volumes of traffic
- Sending malformed TCP/IP packets to a server so that its operating system will crash
- Sending illegal requests to an application to crash it
- Making many processor-intensive requests so that the server's processing resources are fully consumed (e.g., requests that require the server to encrypt each reply)
- Consuming all available disk space by creating many large files.

The checklist in Table 5 provides the major steps to be performed in handling a DoS incident. Note that the exact sequence of steps may vary based on the nature of individual incidents, and on the strategies chosen by the organization for halting DoS attacks that are in progress.

Denial of Service Incident Handling Checklist		
	Action	Completed
	Detection and Analysis	
1.	Prioritize handling the incident based on the business impact	
1.1	Identify which resources have been affected and forecast which resources will be affected	
1.2	Estimate the current and potential technical effect of the incident	
1.3	Find the appropriate cell(s) in the prioritization matrix based on the technical effect and affected resources	
2.	Report the incident to the appropriate internal personnel and external organizations	
	Containment, Eradication, and Recovery	
3.	Acquire, preserve, secure, and document evidence	
4.	Contain the incident—halt the DoS if it has not already stopped	
4.1	Identify and mitigate all vulnerabilities that were used	
4.2	If not yet contained, implement filtering based on the characteristics of the attack, if feasible	
4.3	If not yet contained, contact the ISP for assistance in filtering the attack	
4.4	If not yet contained, relocate the target	
5.	Eradicate the incident; if Step 4.1 was not performed, identify and mitigate all vulnerabilities that were used	
6.	Recover from the incident	
6.1	Return affected systems to an operationally ready state	
6.2	Confirm that the affected systems are functioning normally	
6.3	If necessary and feasible, implement additional monitoring to look for future related activity	
	Post-Incident Activity	
7.	Create a follow-up report	
8.	Hold a lessons learned meeting	

Table 5: Denial of Service Incident Handling Checklist.

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000154

5.3 Malicious Code Incident Handling

Malicious code refers to a program that is covertly inserted into another program with the intent to destroy data, run destructive or intrusive programs, or otherwise compromise the security or integrity of the victim's data. Generally, malicious code is designed to perform these nefarious functions without the system's user knowledge. Malicious code attacks can be divided into five categories: viruses, Trojan horses, worms, mobile code, and blended.

The checklist in Table 6 provides the major steps to be performed in handling a malicious code incident. This checklist is a continuation of Table 3, Initial Incident Handling Checklist. Note that the exact sequence of steps may vary based on the nature of individual incidents and the strategies chosen by the organization for containing incidents.

	Action	Completed
	Detection and Analysis	
1.	Prioritize the handling of the incident based on business impact.	
1.1	Identify which resources have been affected and forecast which resources will be affected.	
1.2	Estimate the current and potential technical effect of the incident.	
1.3	Find the appropriate cell(s) in the prioritization matrix, based on the technical effect and affected resources.	
2.	Report the incident to the appropriate internal personnel and external organizations.	
	Containment, Eradication, and Recovery	
3.	Contain the incident	
3.1	Identify infected systems	
3.2	If the malicious binary has not already been recovered, attempt to recover through forensics.	
3.3	Disconnect infected systems from the network	
3.4	Mitigate vulnerabilities that were exploited by the malicious code.	
3.5	If necessary, block the transmission mechanisms for the malicious code	
4.	Eradicate the incident	
4.1	Disinfect, quarantine, delete, and replace infected files	
4.2	Mitigate the exploited vulnerabilities for other hosts within the organization	
5.	Recover from the incident	
5.1	Confirm that the affected systems are functioning normally	
5.2	If necessary, implement additional monitoring to look for future related activity.	
	Post-Incident Activity	
6.	Create a follow-up report	
7.	Hold a lessons learned meeting	

Table 6: Malicious Code Incident Handling Checklist.

5.4 Unauthorized Access Incident Handling

An unauthorized access incident occurs when a user gains access to resources that the user was not intended to have. Unauthorized access is typically gained through the exploitation of operating system or application vulnerabilities, the acquisition of usernames and passwords, or social engineering. Attackers may acquire limited access through one vulnerability, and use that access to attack through other vulnerabilities, eventually gaining higher levels of access. Examples of unauthorized access incidents include:

- Performing a remote root compromise of an e-mail server
- Defacing a Web server
- Guessing and cracking passwords
- Copying a database containing credit card numbers
- Viewing sensitive data, including payroll records and medical information, without authorization
- Running a packet sniffer on a workstation to capture usernames and passwords
- Using a permission error on an anonymous FTP server to distribute pirated software and music files
- Dialing into an unsecured modem and gaining internal network access
- Posing as an executive, calling the help desk, resetting the executive's e-mail password, and learning the new password
- Using an unattended, logged-in workstation without permission.

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000155

The checklist in Table 6 provides the major steps to be performed in handling an unauthorized access incident. This checklist is a continuation of the Initial Incident Handling Checklist in Table 3. Note that the exact sequence of steps may vary based on the nature of individual incidents and on the strategies chosen by the organization for containing incidents.

Unauthorized Access Incident Handling Checklist		
	Action	Completed
	Detection and Analysis	
1.	Prioritize handling the incident based on the business impact	
1.1	Identify which resources have been affected and forecast which resources will be affected	
1.2	Estimate the current and potential technical effect of the incident	
1.3	Find the appropriate cell(s) in the prioritization matrix based on the technical effect and affected resources	
2.	Report the incident to the appropriate internal personnel and external organizations	
	Containment, Eradication, and Recovery	
3.	Perform an initial containment of the incident.	
4.	Acquire, preserve, secure, and document evidence	
5.	Confirm the containment of the incident	
5.1	Further analyze the incident and determine if containment was sufficient (including checking other systems for signs of intrusion)	
5.2	Implement additional containment measures if necessary	
6.	Eradicate the incident	
6.1	Identify and mitigate all vulnerabilities that were exploited	
6.2	Remove components of the incident from systems	
7.	Recover from the incident	
6.1	Return affected systems to an operationally ready state	
6.2	Confirm that the affected systems are functioning normally	
6.3	If necessary and feasible, implement additional monitoring to look for future related activity	
	Post-Incident Activity	
7.	Create a follow-up report	
8.	Hold a lessons learned meeting	

Table 7: Malicious Code Incident Handling Checklist.

5.5 Inappropriate Usage Incident

An inappropriate usage incident occurs when a user performs actions that violate acceptable computing use policies. Although such incidents are often not security related, handling them is very similar to handling security-related incidents. Examples of incidents a team might handle include users who:

- Download password cracking tools or pornography
- Send spam promoting a personal business
- E-mail harassing messages to coworkers
- Set up an unauthorized Web site on one of the organization's computers
- Use file or music sharing services to acquire or distribute pirated materials
- Transfer sensitive materials from the organization to external locations.

Certain inappropriate usage incidents are more challenging to handle because they are targeted at outside parties. Of course, this raises liability concerns. What makes these incidents particularly interesting is that in some cases, the organization is not actually the source of the attacks—but it appears to outside parties that the organization attacked them. The handlers should work quickly to investigate the activity, collect evidence, and determine if the activity originated from the organization's networks or systems. Examples of inappropriate usage incidents directed at outside parties include:

- An internal user defacing another organization's public Web site
- An internal user purchasing items from online retailers with stolen credit card numbers
- A third party sending spam e-mails with spoofed source e-mail addresses that appear to belong to the organization
- A third party performing a DoS against an organization by generating packets with spoofed source IP addresses that belong to the organization.

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000156

The checklist in Table 8 provides the major steps to be performed in handling an inappropriate usage incident. This checklist is a continuation of the Initial Incident Handling Checklist in Table 3. Note that the sequence of steps may vary based on the nature of individual incidents.

Inappropriate Usage Incident Handling Checklist		
	Action	Completed
	Detection and Analysis	
1.	Prioritize the handling of the incident based on business impact.	
1.1	Determine whether the activity seems criminal in nature	
1.2	Forecast how severely the organization's reputation may be damaged	
1.3	Find the appropriate cell(s) in the prioritization matrix, based on the criminality and damage to reputation	
2.	Report the incident to the appropriate internal personnel and external organizations.	
	Containment, Eradication, and Recovery	
3.	Acquire, preserve, secure, and document evidence	
4.	If necessary, contain and eradicate the incident (e.g., remove inappropriate materials)	
	Post-Incident Activity	
6.	Create a follow-up report	
7.	Hold a lessons learned meeting	

Table 8: Inappropriate Usage Incident Handling Checklist.

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000157

6. Data Investigation Procedures

6.1 Investigations Notification Procedures

When conducting a Security Investigation, it is mandatory to inform anyone we may be contacting of the confidentiality of the investigation, and that the information to be discussed or any facts surrounding the event are not to be shared or discussed with anyone else. Violations of this policy could result in disciplinary action, including termination.

- **Individual Interviews:**

1. Prior to discussing the investigation with anyone or asking questions pertaining to an investigation, the following return receipt email must be sent to the participant:

To: Name
From: Name. Equifax Security
Subject: Important Confidentiality Notice

This is to inform you that I may be contacting you regarding an investigation Equifax Security is conducting. You are hereby notified that any information related to this call, as well as information discussed on the call is confidential. You are prohibited from discussing this matter with anyone in any verbal or written manner. If you are contacted by anyone outside of Equifax Security regarding this issue, you are not to discuss it with them, and you must contact me immediately. Violations of this policy could result in disciplinary action, including termination.

2. Set email to a High Priority and prevent email forwarding using Outlook by selecting Options, permissions, and select "DO NOT FORWARD", also select Request a delivery and read Receipt.

3. Capture the return receipt email, export from your mail client, and save as a part of the investigation documentation.

- **Conference Call Briefings:**

1. When scheduling conference calls regarding a suspected Security Event, the following shall include in the body of the calendar invitation:

You have been invited to participant on a call as part of an incident response team, of which I am the lead investigator. You are hereby notified that any information related to this call, as well as information discussed on the call is confidential. You are prohibited from discussing this matter with anyone in a verbal or written manner. If you are contacted by anyone outside of Equifax Security regarding this issue, you are not to discuss it with them, and you must contact me immediately. Violations of this policy could result in disciplinary action, including termination.

2. Prior to beginning the call, the following statement shall be read to the participants:

Thank you for participating on this call. I need to remind you that any information to be discussed is confidential, and you are prohibited from discussing this matter with anyone. If you are contacted by anyone outside of Equifax Security regarding this issue, you are not to discuss it with them, and you must contact me immediately.

3. Document that the statement was read to all participants as a part of the investigation notes.

6.2 Credit File Investigations Procedures

1. Notification of a security event is received: Customer; consumer; law enforcement; Sales; Customer Service; Security audit monitoring reports.

2. Evaluate situation and determine type of event
   - Internal User
     - Unauthorized Access
     - Unauthorized Access and alteration
   - External customer access, customer data
     - Customer access attempt – ePORT international IP
     - Customer access unauthorized
     - PSOL

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000158

3. Obtain details available concerning the event:
    - Internal
        - Determine User and location
        - Review user activity and conduct investigation
        - Block credit files if file alteration has occurred
    - External
        - Customer user access (known or unknown threat)
        - Customer Name
        - Address
        - Customer Number (s)
        - Website
        - Sales Agent
        - Date(s) of the incident
        - Suspect(s) name and other available information
        - Date of notification
        - Security Digits
            - If suspend, when and by whom?
            - If changed, when and by whom?
        - Order data sets / print and block/ vip potential victims credit file.
        - Analyze credit files for potential fraud characteristics
        - Number of consumers involved and the states of residence
        - Law Enforcement agency involved
            - Name of Detective/ Agent and telephone number
            - Police report

4. Enter into Security Case Log (Appendix D, E).
5. Conduct searches and scans for additional information
    - CIS for additional customer numbers
    - Google
    - Yahoo
    - Accurint
    - Datasets
    - Invoices
    - DataQA tape activity
6. Audit customer
7. Notifications
    - Incident Response team
    - Manager(s)
    - Reseller Alert
    - Sales
    - Customers
    - Consumers
    - Law Enforcement
    - Enter into Decline Database

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000159

8. Finalization
    - Termination
    - Reinstatement of account
    - Consumer Letters

6.3 Reseller Investigation Procedures

1. Security is notified of event: Reseller; customer; law enforcement; monitoring reports
2. Obtain from reseller details needed to begin investigation:
    - A summary of the incident, listing all contact information for the parties involved.
    - If subscribers or other companies are involved, list all company names, addresses, and contact information.
    - Date that the event occurred
    - Date access to Equifax information was suspended
    - Who suspended the access
    - Number of consumers affected by the event
    - List of the consumers affected by the event
3. Law enforcement (if more than one agency is involved, include the following for each):
    - Date law enforcement was notified
    - Name and location of the agency
    - Name and contact information of the investigator
    - Include a copy of the police report
4. Consumer notification letter:
    - Date notification letter mailed
    - Include a copy of the letter for Equifax review prior to release
    - Include consumer monitoring services to "Affected consumers"
5. Enter into Security Case Log (Appendix C, D)

6.4 PSOL Investigation Procedures

1. Receive notification of a security event:
    - Consumer complaint of unauthorized PSOL, FACT or AA access
    - Consumer complaint of unauthorized credit card use
    - Operator suspicion of consumer fraudulent activity
    - Monitoring reports
    - Law enforcement subpoena
    - Law enforcement contact.

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000160

2. Identify details of event by accessing Seibel:
    - Review call notes and log
    - Review order history
    - Review IP address
    - Review credit card history
3. Additional investigation via Accurint, Google, or other tools
4. If necessary, submit fraud query for additional information
5. For consumer complaints or operator suspicions: Respond to PSOL supervisor with results of investigation
6. For law enforcement subpoenas:
    - Print documents requested and redact proprietary Equifax information such as EID score and EID reason codes
    - Prepare letter to law enforcement verifying compliance with subpoena
    - Sign certification, if provided
    - Fax or over-night records in response to the subpoena
7. For law enforcement contact:
    - Conduct investigation to determine what information can be provided to law enforcement
    - Direct law enforcement on subpoena process
8. For large scale PSOL investigations:
    - Notify Incident Response Team
    - Determine law enforcement involvement
9. Report and track incident in Intellinx Case Manager (Appendix D. E)

6.5 Phishing Response Procedures

These procedures detail the steps necessary to quickly and effectively respond to phishing attacks against Equifax portals.

1. Notification – Notification of a phishing attack may come through various vectors. These include:
    - Internet Identity (II). II will contact Nicole Smith & Nick Nedostup. (Internet Identity is Equifax's third party vendor who monitors for phishing attacks against Equifax websites).
    - NDR Monitoring. A custom script has been deployed on Equifax's Brightmail server. This script monitors for a spike in Non Deliverable Email. Large spikes can be an indicator of a phishing attack.
    - FraudWatch. Our FraudWatch program reviews websites and sites that report phishing emails for phishing attacks against Equifax.
    - Customer Notification. In some cases, a customer may be the first to contact us, asking if an email is legitimate.
2. Initial Alert – For all potential attacks, regardless of notification vector, the following personnel should be notified: Cyber Threat Center On-Call - [HYPERLINK "mailto:security.incident@equifax.com" \h] **,+1 678-795-7106** or **1- 888-257-8799** and **press 1** for *Security Incident*
3. Verification – After notification the phishing attack is verified:
    - Review and report by Security Operation's response team.
    - Review and report by Internet Identity.
4. Internet Identity Shutdown authorization: Authorize Internet Identity to perform shutdown of all related phishing sites.

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000161

5. Management Alert
    - Immediately upon confirming that a phishing attack has occurred, the Vice President of Security Investigations is to be notified.
    - Next, include the following personnel in a meeting/phone bridge to review the attack and approve appropriate response measures:
        - Greg Baker, VP Global Corporate Security & Safety
        - Nicole Smith, Sr. Director Investigations
        - Adam Magill, VP Cyber Threat Center
        - Tim Klein, Media Relations
        - Diane Bernez/Sty Carter, Communications
        - Greg Wagner, Lotus Notes
        - Ann Hester, Help Desk
        - Richard Goerss, Legal
        - Business contact for the portal attacked (APPENDIX F)
        - Technical contact for the portal attacked (APPENDIX F)
6. Alert Internal Personnel
    - Brief Executive Management on attack and response procedures.
    - Inform the appropriate Help Desk regarding phishing attack so that they can answer customer questions:
        - Instruct the help desk to immediately inform Nicole Smith of any customer who say they fell victim to the attack
        - Instruct the help desk to immediately change the logins and passwords of any customers who say they fell victim to the attack.
    - Inform appropriate business and sales team of the affected portal so they can answer customer questions.
7. Alert Customers
    - Place a high profile alert on the affected portals webpage/login page.
    - Contact Information in (APPENDIX F)
    - Determine if it is effective and feasible to email customers of the affected portal.
    - Place an alert on the main Equifax web page
8. Have the technical team and Internet Identity collect samples for review
    - Sample NDR emails
    - Sample of web server logs
    - Email's reported to abuse sites
    - Internet Identity provided websites and emails
    - Help Desk provides samples from customers
9. Monitor phishing websites for changes or adaptations
10. Analyze access patterns of victimized customers: Analyze access patterns of all customers for similarities to victimized customers i.e. access from the same IP address

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000162

6.6 Evidence Handling Procedures

The following are the evidence handling procedures and guidelines followed by EFX in regards to digital and computer evidence. EFX follows current industry best practices for handling and securing digital evidence, and this document is periodically updated reflect these practices. These procedures and guidelines, while covering the most common areas of evidence handling, are neither all-inclusive nor a mandate, as each investigation may require a unique approach as agreed upon by all parties.

- **Evidence Acquisition**

All digital evidence must be acquired in a manner that preserves the integrity of that evidence. Original evidence should be secured and proper chain of custody created (Appendix G). Forensic copies of the original should be created for use in the examination.

- Non-volatile evidence (i.e. hard drives or memory cards) is best acquired at a bit level using forensically sound software, a hardware write blocker, and a trusted system. All copies should be verified as exact copies of the original through the use of mathematical hashes such as MD5 and SHA1.
- In cases where the above isn't feasible and the risk is acceptable, other methods of acquisition such as booting to alternate media, acquisition of live a system, or partial imaging may be performed by those trained and/or experienced in these various techniques.
- Volatile evidence, when necessary to the investigation, is best acquired immediately using known trusted static binaries or software running from alternate media by those trained and/or experienced in this type of acquisition.

- **Evidence Transfer**

All digital evidence must be transferred in a manner that preserves the integrity of the evidence and maintains a proper chain of custody. Additionally, the method of transfer should be appropriate based on the sensitivity of the data.

- Evidence should be shipped in a manner that protects it from damage. I.e. Use sufficient packaging materials that are anti-static in nature.
- Evidence is best shipped double-boxed with the inner box sealed to detect tampering. I.e. Sealing the inner box with evidence tape or using regular tape and initialing across the tape seals.
- Evidence is best shipped requiring the direct signature of the receiving person for delivery.
- Non-sensitive evidence (log files, no personal data, etc…) may be shipped through FedEx without additional protections.
- Sensitive evidence (forensic images including personal or business data) is best encrypted before shipping with FedEx to provide additional protection.
- Critical evidence (original evidence, very sensitive personal or business data, etc…) is best delivered using Brinks secured courier or hand delivered to or picked up by EFX personnel.

- **Evidence Storage**

All digital evidence must be stored in a manner that ensures the integrity and confidentiality of that evidence.

- Evidence should be stored in a secure location that ensures it will remain inaccessible to anyone un-authorized.
- All evidence is best stored locked in a dedicated safe or inside a secured room.
- Minimally, devices directly containing digital evidence (hard drives, CDs, DVDs, memory sticks, etc…) should be stored locked in a dedicated safe or secured room.
- Storage of devices containing volatile evidence (pagers, cell phones, memory, etc…) should be done in a manner that maintains power to the devices preventing the loss of evidence.

- **Evidence Disposal**

Evidence should be disposed of only after ensuring it will be no longer needed for any civil, criminal, or administrative action. Normally, digital evidence is returned in the exact state it was received.

- Long term storage of digital evidence may be arranged in a secure location.
- Upon request, digital evidence may also be disposed of by:
  - Logical destruction – repeatedly overwriting the media the evidence resides on with random data
  - Physical destruction – physically destroying the media the evidence resides on.

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000163

6.7 Evidence Shipping Procedures

This procedure is designed to ensure secure shipment of potentially sensitive evidence.

- **Notes:**

Original evidence is not shipped overseas without written approval from a VP in the security organization. The original evidence should be secured onsite and an encrypted forensic image of the evidence should be shipped.

- **Required:**
  - Forensic image of original evidence
  - File containing MD5 and/or SHA1 hashes of the evidence file(s)
  - Encryption software (minimum AES or 3DES with 128bit key)
  - Anti-static packing materials to double-box the evidence
  - EFX Evidence Custody Form
- **Warnings:**
  - Never ship any sensitive or potentially sensitive evidence unencrypted.
  - Ensure MD5 and/or SHA1 hashes are taken of the evidence pre-encryption and included in the shipped data.
- **Procedure:**
  1. Ensure that the original evidence is locally secured with an EFX Evidence Custody Form.
  2. Ensure that a forensic image of the original evidence is maintained.
  3. Create MD5 and/or SHA1 hashes of the evidence file(s) and save these to a text file.
     - Large numbers of files may be zipped or archived together before taking MD5/SHA1 hashes.
     - Include copies of all imaging notes and/or audit logs
     - Encrypt all forensic image files and documentation/audit files with an appropriate level of encryption[2]
  4. Ensure that EFX has the appropriate software to decrypt to evidence.
  5. Either encrypt the file individually on unencrypted media OR
  6. Move the files onto encrypted media (i.e. encrypted hard drive or backup tape)
  7. Fill out an Evidence Custody Form (Appendix G) for the encrypted data and place that form in the package with the media.
  8. Package the media to be transferred in safe, anti-static packaging and seal the package closed with tape.
  9. Sign your name across the tape such that one-half of your signature is on the tape and one-half is on the package itself.
  10. Ship evidence - ship the evidence package, requiring signatures, to:

      Nicole Smith
      Equifax Inc
      Mail Drop: NP41 1110 Abernathy Road
      Atlanta, GA 30328

  11. Email the tracking number and encryption password to [HYPERLINK "mailto:nicole.smith@equifax.com" \h]

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000164

6.8 Remote Imaging Procedures

This procedure is designed to assist non-forensic personnel in creating forensic images of PCs in a manner that can be successfully examined by EFX computer forensic analysts.

- **Notes:**

This procedure relies on imaging a live running system, collecting volatile data and creating a full disk image from that system. This live imaging procedure is used for remote imaging in cases where it is not practical to get a forensic examiner onsite and when it is not practical to ship the original drive. It should not be used without prior approval of an EFX forensic examiner. The Equifax preferred remote imaging process includes the use of EnCase Enterprise. EnCase Enterprise will allow the remote preview and acquisition of evidence with minimal modification of the suspect system.

- **Required:**
    - Access (remote or physical) to the suspect system and administrative credentials that will allow the installation of software.
    - A copy of the latest EnCase Enterprise Servlet for Equifax (network path to latest official servlet).
    - Connected to the network over an Ethernet cable (VPN and Wi-Fi are also possible but not preferred).
    - The ability to connect over the network to the EnCase Enterprise Authentication Server (172.26.2.12) on TCP port 5818.
    - Connected to a power source in a secure location.
    - The ability to secure the suspect system overnight where it is protected from tampering and disconnection.
- **Warnings:**
    - If the system is suspected of being infected with Malware, then the credentials used on the system should be considered compromised.
    - If the system user has Administrator level access the servlet should be installed using that account as those credentials are likely already compromised if malicious software is on the system.
    - If a separate administrator account is needed to install the servlet the password should be changed immediately after the install process is completed. The password should be changed on a different system than the suspect system.
- **Procedure:**
    - Identify the system name and IP address of the suspicious activity or system used by subject/user.
    - Connect or verify system is connected to the EFX network.
    - Verify that the system is connected to a power source that will not be disconnected.
    - At no point is it permissible to connect any other devices to the system ports unless specifically instructed by the requester.
    - Use a cable lock or other security method to protect the device from theft while imaging (this could run overnight or over days).
    - Contact Asif Ansari for boxes in STL and Amit Garg for all other locations requesting that the EnCase Servlet be deployed to the systems using SCCM.

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000165

- In the event that the servlet cannot be deployed using SCCM, the Servlet will need to be installed manually:
  - If the user is aware or can be made aware, the servlet can be provided to the user via network share or over Microsoft Lync and instructed to install the servlet.
  - If the user is not aware, Local IT can install the servlet to the system from a network share or optical media.
  - Once the servlet is installed, open a terminal window (CMD) and check for a successful ping of 172.26.2.12 and report back to requester (Forensic Examiner).
- Open task manager and on the Processes tab click "Show processes from all users" then verify that enstart.exe or enstart64.exe is running on the system.
- Report this information back to the requester (Forensic Examiner).
- The forensic examiner will verify connectivity and at that point the system screen can be locked.

6.9 Lost/Stolen Asset Investigation Procedures

1. Notification of lost or stolen asset (laptop, Blackberry) is received from Cyber Threat Center or Asset Incident:
   - Lost or stolen assets should be reported 24 hours a day to 1-800-456-7152 or 1- 770-740-4357 or via email to Asset Incident
   - Lost or stolen assets should also be reported to [HYPERLINK "mailto:Security.Operations@equifax.com" \n]or 1-888-257-8799 or 1-770-740-6072
2. Contact employee or contractor and obtain the following information:
   - Date, time and location of loss
   - Details of loss
   - Police report number and contact information – also request copy of police report when available
   - Determine if VPN token was lost
   - Determine if asset contained consumer or sensitive data
   - Verify laptop was encrypted
   - Determine if passwords or sensitive data were located with the laptop
   - Verify no other EFX asset was lost
3. Verify network ID, VPN token and passwords have all been disabled
4. Prepare Security Incident Report (Appendix H)
5. Transmit incident report to Vice President Investigations and Chief Security Officer
6. Follow-up with employee until police report is provided for records
7. Report incident in Intellinx Case Manager (Appendix D)

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000166

7. Security Event Consumer Notification Procedures

7.1 Consumer Notification Procedures

- Notices to consumers may be delayed if an appropriate law enforcement agency determines that consumer notification will interfere with a criminal investigation and provides Equifax with a written request, or an oral request to be followed by a written request, for the delay;
- "Affected consumers", to whom notices will be provided, are consumers to whom substantial harm or inconvenience could result due to the unauthorized access or use of their "sensitive consumer information". For these purposes," sensitive consumer information" means a consumer's name, address, or telephone number, in conjunction with the consumer's social security number, driver's license number, account number, credit or debit card number, or a personal identification number or password that would permit access to the consumer's account. "sensitive consumer information" also includes any combination of components of customer information that would allow someone to log onto or access the consumer's accounts, such as user name and password or password and account number.
- So as not to unnecessarily alarm consumers, notices will be limited to those consumers who Equifax determined that misuse of their information has occurred or is reasonably possible. If Equifax determines that a group of files were accessed improperly, but is unable to determine the specific consumer information that was accessed, but that misuse of whatever information was accessed is possible, Equifax will notify all consumers in the group;
- Supervise the contents and delivery of the notice to the "Affected consumers". The notice will:
    - Be provided in a clear and conspicuous manner, either by telephone or in writing
    - Will describe the incident in general terms and identify the type of consumer information that was the subject of the unauthorized access or use
    - Will describe what Equifax has done to protect the consumer's information from further unauthorized access, such as taking their credit file off-line, and with the consumer's agreement, replace the file block with a fraud alert
    - Include a toll-free telephone number that consumers can call for further information and assistance
    - Remind consumers of the need to review their account statements and their credit files at all three nationwide consumer reporting agencies;
    - Advise consumers:
        - How to obtain copies of their credit file from each of three nationwide consumer credit reporting agencies;
        - To report any suspicious information to the consumer reporting agency
        - How to remove any unauthorized inquiries to their credit file
        - About adding fraud alerts to their credit files,
        - Advise consumers to report any suspicious activity to law enforcement;
    - Advise consumers how to receive free credit monitoring services of the Equifax credit file
    - Provide information from the FTC about how to protect against identity theft by providing the FTC's web site address and toll-free telephone number to obtain identity theft guidance and report suspected incidents of identity theft;
    - Also contain any additional information that may be required by state security breach notice laws;
- Notify Experian and TransUnion if notices will be sent to more than 1,000 "Affected consumers", if the notices include their contact information.

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000167

7.2 Law Enforcement Notification

*Only provide necessary data as approved by Management

- **Phishing Attack:** Notify FBI Atlanta
- **Consumer Data Internal**
    - For fraud involving mail or across any form of wire communication like telephone, fax, etc.:
        - Notify United States Postal Service (USPIS) in state where fraud occurred, suspect resides, or victim resides
        - Jurisdiction requires interstate action by suspect
        - Victim/monetary guideline minimums which can be obtained from USPIS contact
    - For fraud involving credit cards, monetary transfers, etc:
        - Notify US Secret Service (USSS) in state where fraud occurred, suspect resides, or victim resides
        - Jurisdiction requires interstate action by suspect
        - Victim/monetary guideline minimums which can be obtained from USSS contact
- **Unknown External Threat**
    - For fraud involving any type of external threats like phishing, hacking, account take- overs, etc.:
        - Notify FBI in state where fraud occurred, suspect resides, or victim resides
        - FBI investigates Jurisdiction requires interstate action by suspect
        - Victim/monetary guideline minimums which can be obtained from USPIS contact
- **Lost Laptops:** Contact police department that took report
- **Sources for Contacting Law Enforcement:**
    - Equifax Security Contact Database
    - CFE Database
    - IAFCI Database

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000168

8. Physical Security Event Procedures

8.1 Overview

The development and testing of procedures to be followed in case of extreme emergencies such as fire, tornadoes, hurricanes, medical, bomb threats

8.2 General Procedures

A number of employees within Equifax have been selected as "Crisis Managers/Leaders to ensure a timely evacuation and/or shelter in the event of fire, tornado or bomb threat.

All Crisis Leaders have an emergency manual that explains their responsibilities.

Evacuation maps and procedures are posted on walls throughout the building. Employees should familiarize themselves with the evacuation route from all areas of the facility.

8.3 Crisis Leader/Manager Responsibilities

During emergency evacuations, ensure that all personnel proceed to exits as quickly and safely as possible. Direct all personnel to walk on the right side of all hallways and stairwells.

Ensure that all personnel have evacuated your area of responsibility. Check offices, copy and print rooms, restrooms and conference rooms. If there is a hearing-impaired employee in your area, be sure they are aware of the emergency.

8.4 Fire Procedure

If there is a fire in your area, notify Security Command Center. Identify the floor location and the severity of the fire. Contact Security or Facilities Management to call the fire department.

Actual Fire (Visible)

1. Evacuate your building area.
2. Use the evacuation process found in Crisis Plan.
3. Call 911 giving the address, location, and situation.

8.5 Tornado Procedure

In the event of a tornado, make sure no one goes outside of the building. Keep everyone away from windows and lobby areas.

8.6 Bomb Threat Procedure

In the event of a Bomb Threat have employees quickly check around their area for unfamiliar items before evacuation. Inform the employee: **IF AN ITEM IS FOUND, DO NOT TOUCH IT!**

1. Keep the individual on the telephone.
2. Gather as much information about the bomb as possible.
3. If a BOMB Threat is received, immediately notify Security Command Center.
4. The directive to activate the Building Fire alarm for evacuation will be given at that time.
5. Evacuate per local Crisis Plan.

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000169

8.7 Medical Emergency Procedure

1. Call 911 and remain with victim until Medical Team arrives.
2. Collect all information necessary to help with the medical emergency.

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000170

Appendix A - Definitions

Adware – Any software application, which displays advertising banners while running a program. Adware includes additional code that delivers the ads, which can be viewed through pop-up windows or through a bar that appears on the computer screen. It usually includes code that tracks a user's personal information and passes it on to third parties without the user's authorization or knowledge.

Botnet – A network of compromised machines that can be remotely controlled by an attacker. Due to their immense size (tens of thousands of systems that can be linked together), they pose a severe threat to the Company's IT infrastructure.

Breach - Any illegal penetration or unauthorized access to a computer system that causes damage or has the potential to cause damage.

Chain of Custody - Protection of evidence by each responsible party to ensure against loss, breakage, alteration or unauthorized handling. Protection also includes properly securing, identifying, and dating evidence.

Compromise –The unauthorized disclosure, modification, substitution, or use of sensitive information or the successful action to invade system by getting around security. A computer has been compromised, for example, when a Trojan Horse has been installed.

Compromise of Integrity –Any unauthorized modification of information or data.

Cyber/Computer Security Incident – A violation or imminent threat of violation of computer security policies, acceptable uses or standard computer security policies. It is also any adverse event whereby some aspect of a computer system is compromised as: loss of data confidentiality; disruption of data integrity; disruption of availability, also known as a denial of service.

Damage –The unauthorized deliberate or accidental physical or logical modification, destruction or removal of information or data from an IT system.

Denial of Service (DoS) – An inability to use system resources due to unavailability; for example, when an attacker has disabled a system, a network worm has saturated network bandwidth, an IP address has been flooded with external messages or the system manager and all other users become locked out of a system.

Event – Any observable or measurable occurrence in a system or network. Events may include, but are not limited to, a user connecting to a file share, a server receiving a request for a Web page, a user sending electronic mail, and firewall blocking a connection attempt.

Evidence – Events, files, logs, messages, items or anything that is used to support an argument.

Finding – An event or occurrence that may cause a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices. Findings require agencies or OCIO CS analysis prior to becoming an incident.

Firewall – A system that controls network traffic between two networks to minimize unauthorized traffic or access. Firewalls can protect networks and systems from exploitation of inherent vulnerabilities. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet.

Harm – To cause damage, injure or impair IT systems using electronic methods, which can include intangible things such as identity theft.

Incident Closure or Closeout – The last phase of incident handling lifecycle during which the IRT submits the incident report to the CSCO/CTO for review and comment. Closeout is not final until peer review has been completed and all questions regarding the incident are answered satisfactorily.

Incident (Cyber Security) – A violation or imminent threat of violation of computer security policies, acceptable use or standard computer security practices. It is also any adverse event whereby some aspect of a computer system is compromised, such as loss of data confidentiality, disruption of data integrity, disruption or denial of service. The types of incidents are been classified into LOW, MEDIUM or HIGH levels depending on the severity.

Incident Declaration – The phase of the incident handling lifecycle during which a EQUIFAX incident number is assigned and the responsible EQUIFAX organization begins its incident handling process. An incident is declared by a Equifax department, staff office, or incident response team (IRT) that is recognized and documented as being responsible for incident handling.

Incident Handling - The comprehensive management process of receiving incident indications and warnings from Intrusion Protection Systems (IPS), United States Computer Emergency Response Team (US-CERT), law enforcement or Internet Service Providers (ISP) that an incident has occurred. It includes identifying the actual incident type, verifying the victim or perpetrator's responsible company, alerting the company. It also requires reporting, responding to, mitigating and closing a EQUIFAX CS incident.

Incident Notification – This phase of the incident handling lifecycle involves the formal transmission of declared incident information to the documented incident handling or management personnel in the EQUIFAX organization that is experiencing a CS incident.

Incident Oversight – The process of ongoing review and follow-up of incident status by the Equifax incident handling organizations, staff, or assignees to maintain accurate Equifax incident records on the number of incidents declared open closed or cancelled.

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000171

Incident Preparation – This phase of the incident handling lifecycle involves preparing reports and providing continuous status on the incident.

Incident Prevention – This phase of the incident handling lifecycle involves the review of alerts, warnings and suspected events from various sources. In addition, it involves continuous system monitoring and review of risk assessments for systems with high CS incident rates.

Incident Reporting - This phase involves a formal acknowledgement by the Equifax incident handler that a CS incident has occurred and that notification of all personnel responsible for responding to, acting upon, or resolving an incident have been notified. The incident reporting process includes notification of the CSCO.

Incident Response – The process of acting upon known identified incidents. The process includes analysis of how the incident occurred, actions to contain the incident, eradicate the cause of the incident, repair the damage, and recover from the incident. This phase includes collection and preparation of a lessons learned report and assistance in the development of an incident report.

Incident Tracking – The process and requirement for Equifax to maintain comprehensive records of all incidents from the time of declaration through closure.

Intrusion – An unauthorized, inappropriate or illegal activity by insiders or outsiders that can be considered a penetration of a system.

Intruder - A person who is the perpetrator of a computer security incident. Intruders are often referred to as —hackers or —crackers. Hackers are highly technical experts who penetrated computer systems; the term crackers refer to the experts with the ability to —crack computer systems and security barriers. Most of the time —cracker is used to refer to more notorious intruders and computer criminals. An intruder is a vandal who may be operating from within Equifax or attacking from the outside.

Level of Consequence - The impact an incident has on an organization. Impact includes: loss of data; the cost to a Equifax company or mission area; negative consequences to the organization (e.g. damage to reputation); and the magnitude of damage that must be corrected.

Malicious Code – Also known as —Malware (malicious software), is a computer code or program designed to deny, destroy, modify, or impede a system's configuration, programs, data files, or routines. Malicious code comes in several forms, including viruses and worms.

Misuse - Unauthorized use of an account, computer or network by an intruder or malicious user (or insider).

Need-to-Know - The necessity for access to, knowledge of, or possession of classified or other sensitive information in order to carry out officially sanctioned duties. Responsibility for determining whether a person's duties require possession or access to this information rests upon the individual having current possession (or ownership) of the information involved, and not upon the prospective recipient. This principle is applicable whether the prospective recipient is an individual or contractor.

Pharming – An exploit of the Domain Name Server (DNS) that tries to or actually transforms the legitimate host name into another IP address. The "pharmer" sets up a website looking similar to
a legitimate site and harvests personal information from unsuspecting users. Also known as —DNS cache poisoning.

Phishing – An exploit that imitates legitimate companies' e-mails to entice people to reveal sensitive or private information, or creates a replica of an existing web page to fool a user into submitting personal, financial or password data.

Rootkit – A set of tools used by an attacker after gaining root-level access to a host to conceal the attacker's activities on the host and permit the attacker to maintain root-level access to the host through covert means.

Spyware - Any technology that aids in gathering information about a person or organization without their knowledge. Sometimes this software is called a "spybot" or —tracking software. Spyware is put in someone's computer to secretly gather information about the user or company and relay it to advertisers, foreign companies, and other interested parties. Spyware can be installed as part of a virus, worm, or result from installation of a program. Spyware is often installed without the user's consent as a drive-by download, by clicking on some option of a deceptive pop-up or webpage, adware or e-mail attachment.

Threat –A circumstance, condition, or event with the potential to cause harm to personnel and/or network resources in the form of destruction, disclosure, modification of data, DoS, and/or fraud, waste and abuse. The most common security threats are to network systems. Network security threats include impersonation, eavesdropping, DoS, packet replay/modification.

Trojan Horse – A non-self-replicating program that seems to have a useful purpose, but in reality has a different malicious purpose.

Virus – A small piece of malicious code that attaches itself to another program. It does not run on its own, but executes when the host program is run.

Worm – A type of malicious code that acts as an independent program, and can usually replicate itself without human interaction from one system to another.

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000172

Appendix B - Abbreviations

ACRO	Automated Credit Reporting System
ACIS	Automated Consumer Information System
AUD	Automated Universal Data System
ACDV	Automated Consumer Dispute Verification
CDIA	Consumer Data Industry Association
CIO	Chief Information Officer
CIS	Customer Information System
CRA	Consumer Reporting Agency
CS	Cyber Security
CSCO	Chief Security and Compliance Officer
CTC	Cyber Threat Center
ESIRT	Equifax Security Incident Response Team
DCAT	Customer Attribute Table
DNS	Domain Name Server
DoS	Denial of Service
EFX	Equifax
EMS	Equifax Mortgage Services
e-OSCAR	Electronic Online Solution for Complete and Accurate Reporting
FCRA	Fair Credit Reporting Act
FTP	File Transfer Protocol
IHT	Incident Handling Team
IP	Internet Protocol
IPS	Intrusion Prevention System
IR	Incident Response
ISP	Internet Service Provider
IT	Information Technology
ITN	Incident Ticket Number
MSSP	Managed Security Services Provider
POA	Plan of Action
POC	Point of Contact
PSOL	Personal Solutions
SA	System Administrator
SOC	Security Operations Center
US-CERT	United States Computer Emergency Response Team
VP CTC	Vice President, Cyber Threat Center

Table B-1: List of common abbreviations.

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000173

Appendix C – Incident Classification Matrix

Characteristics	Severity Determination			
	SEV4 (Informational)	SEV3 (Warning)	SEV2 (Severe)	SEV1 (Critical)
Sensitivity of Asset	Non-critical	Non-critical	Critical	Critical
Sensitivity of Data	Public	For Internal Use Only	Confidential and higher	Confidential and higher
Interruption of Service	None or some internal	Brief	Brief (<4 hours)	Extended (>4 hours)
Expert Assistance	None	Internal	Internal or external	Internal or external
Reporting SLA's				
Notify Business Owner	Monthly	Weekly	4 hours	1 hour
Notify Custodian	Weekly	Daily	2 hours	1 hour
Notify CSCO	Monthly	4 hours	2 hours	1 hour
Computer Incident Update Meetings	Weekly	Daily until contained. Weekly during business hours to close.	Every 4 hours until contained. Every other day during business hours to close.	Every 2 hours until contained. Daily during business hours to close.
Data Incident Update Meetings	N/A	As needed.	Weekly until resolved.	Daily until resolved.

Table C-1: Incident Classification Matrix.

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000174

Appendix D – Archer Ticketing System

The Archer ticketing system shall be used for documenting of all Security Incidents. The fields and logic are constructed in such a way that when the information is entered in correctly, all necessary information will be captured at the appropriate steps. The Archer system will use EIS credentials, to appropriately assign permissions granted through Access Manager.

The Archer system can be access by browser from within the Equifax corporate network at:

[HYPERLINK "https://archer.eis.equifax.com/Archer/"]

Screenshots:

Figures D-1 and D-2: Archer instance screen captures demonstrating the "General Information" and "Incidents: Add New Record" fields.

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000175

Appendix E - Internal Security Investigative Worksheet

Note: To be used when Archer is not available.

INTERNAL USER INFORMATION

User's Name: _____ User ID: _____ ACRO _____ ACIS_____

_____Employee: _____ Contractor Date Employed: _____

HR ID #:____ SS#:_____ Dept.:_____

Vendor_____Location: _____

Manager's Name: _____

ACRO Access Type: ____OPTR1 ____OPTR2 ____ONACISM

____ONMTNC1 ____ONMTNC2 ____ONMTNC3 ____ONMTNC4

COMPLAINT INFORMATION

Name: _____ Telephone Number: _____ Email: _____

Address: _____ Employer: _____

Date of Notification: _____ How Notified: _____

Date(s) of Occurrence: _____ Number of Consumers Involved: _____

Security Report: _____

SUSPECT INFORMATION

Name: _____ Telephone Number: _____ Email: _____

Address: _____ Employer: _____

LAW ENFORCEMENT

Agency: _____ Detective: _____ Contacted By: Customer

Telephone Number: _____ Email: _____

SEARCHES

☐ Accurint ☐ Google ☐ Yahoo ☐ IntelliriX ☐ ACRO ☐ ePORT ☐ eID ☐ PSOL

SCANS

☐ Dataset ☐ Print Dumps ☐ Block Files Date: _____

NOTIFICATIONS

☐ Customers ☐ Tiger Team ☐ Decline Database ☐ Major Customers

☐ Sales ☐ Reseller Alert ☐ Law Enforcement

☐ Consumers How: ____ Date: ____

Figure E-1: Internal Security Investigative Worksheet.

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000176

Appendix F - Security Investigative Worksheet

-To be used when Archer is not available.

CUSTOMER INFORMATION

Customer Name:_____ Customer Number: _____
Address:_____ Telephone Number: _____
Contact Name:_____ Title:_____ Email: ___ Website:_____
_____ Date Open:_____ Sales Agent: __
Associated Member Numbers: _____ _____ _____ _____ _____
Security Digits:_____ Suspended: Yes Date:_ Changed: Yes Date:___ By: _____ Reinstated: Yes
Date:_____ Terminated: Yes Date: _____

COMPLAINT INFORMATION

Name:_____ Telephone Number:_____ Email: _____
Address:_____ Employer: _____
Date of Notification:_____ How Notified: _____
Date(s) of Occurrence:_____ Number of Consumers Involved: _____

SUSPECT INFORMATION

Name:_____ Telephone Number:_____ Email: _____
Address:_____ Employer: _____

LAW ENFORCEMENT

Agency:_____ Detective:_____ Contacted By: Customer
Telephone Number:_____ Email: _____

SEARCHES

☐ Accurint ☐ Google ☐ Yahoo

SCANS

☐ Dataset ☐ Print Dumps ☐ Block Files Date: _____

NOTIFICATIONS

☐ Customers ☐ Tiger Team ☐ Decline Database ☐ Major Customers
☐ Sales ☐ Reseller Alert ☐ Law Enforcement
☐ Consumers How: Date:

Figure F-1: Security Investigative Worksheet.

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000177

Appendix G - Evidence/Property Custody Document

EVIDENCE/PROPERTY CUSTODY DOCUMENT For use of this form see Equifax Standard Operating Procedures	CONTRACT DATE OTHER NUMBER
RECEIVING ORGANIZATION Equifax, Inc.	LOCATION 1525 Windward Concourse Alpharetta, GA 30005
NAME AND TITLE OF PERSON FROM WHOM RECEIVED ☐	ADDRESS OF PERSON (Include Zip Code)
PHYSICAL LOCATION FROM WHERE OBTAINED	REASON OBTAINED / TIME/DATE OBTAINED

ITEM NO	QUANTITY	DESCRIPTION OF ARTICLES RECEIVED (Include name, model, serial number, condition and unusual marks)

CHAIN OF CUSTODY				
ITEM NO	DATE	RELEASED BY	RECEIVED BY	PURPOSE OF CHANGE OF
		SIGNATURE NAME AND TITLE	SIGNATURE NAME AND TITLE	
		SIGNATURE NAME AND TITLE	SIGNATURE NAME AND TITLE	
		SIGNATURE NAME AND TITLE	SIGNATURE NAME AND TITLE	
		SIGNATURE NAME AND TITLE	SIGNATURE NAME AND TITLE	
		SIGNATURE NAME AND TITLE	SIGNATURE NAME AND TITLE	

PAGE_____OF _____

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000178

CHAIN OF CUSTODY *(Continued)*				
ITEM NO	DATE	RELEASED BY	RECEIVED BY	PURPOSE OF CHANGE OF CUSTODY
		SIGNATURE	SIGNATURE	
		NAME AND TITLE	NAME AND TITLE	
		SIGNATURE	SIGNATURE	
		NAME AND TITLE	NAME AND TITLE	
		SIGNATURE	SIGNATURE	
		NAME AND TITLE	NAME AND TITLE	
		SIGNATURE	SIGNATURE	
		NAME AND TITLE	NAME AND TITLE	
		SIGNATURE	SIGNATURE	
		NAME AND TITLE	NAME AND TITLE	
		SIGNATURE	SIGNATURE	
		NAME AND TITLE	NAME AND TITLE	
		SIGNATURE	SIGNATURE	
		NAME AND TITLE	NAME AND TITLE	
		SIGNATURE	SIGNATURE	
		NAME AND TITLE	NAME AND TITLE	

FINAL DISPOSITION ACTION

RELEASE TO OWNER OR OTHER

*(Name/Organization)*__ ______________________________________ DESTROY

FINAL DISPOSITION AUTHORITY OR WITNESS

ITEM(S)____________________ ON THIS DOCUMENT, PERTAINING TO THE INCIDENT INVOLVING ____________

____ (IS) (ARE) NO LONGER

(Name) *(Organization/Company)*

REQUIRED AS EVIDENCE AND MAY BE DISPOSED OF AS INDICATED ABOVE. *(If article(s) must be retained, do not sign, but explain in separate correspondence.)*

____

WITNESS TO DESTRUCTION OF EVIDENCE

THE ARTICLE(S) LISTED AS ITEM NUMBER(S) ________________ (WAS) (WERE) DESTROYED BY

____

IN MY PRESENCE, ON THE DATE INDICATED ABOVE

____

PAGE __________ OF __________

Figure G-1: Evidence/Property Custody form.

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000179

Appendix H – Sample Security Incident Report

SECURITY INCIDENT REPORT

TO: VP Global Corporate Security & Safety

FROM: INVESTIGATOR

SUBJECT: JOHN DOE STOLEN LAPTOP

DATE: 10/31/2012

CC: CHIEF SECURITY OFFICER

On January 1, 2009, at approximately 4:00pm, John Doe, (Title), went to the movies. When he returned to his home at approximately 7:00pm, he discovered that the home had been burglarized—the back window had been broken. The home was located at 1234 Nowhere Street, Atlanta, GA 30328. Among the items taken were a TV, camera, iPOD, and his laptop bag. The bag contained his laptop and RSA token. John Doe contacted Fulton County Police Department and filed a report with Detective DoGood, (404) 555-1212. John Doe will provide a copy of the police report when it is available.

John Doe contacted Equifax and reported the loss so that his network ID and password could be deactivated. His RSA token ring was also disabled. The laptop was encrypted. No passwords were located with the laptop. The laptop did not contain any consumer or PII data.

Figure H-1: Example of a Security Incident Report.

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000180

Appendix I - Security Dial in Phone Numbers

Security Management Bridge
Toll: 1-719-387-5597
Toll Free: 1-866-628-8620
Participant Code: Redacted

Security Conference (Technical) Bridge
Toll: 1-719-234-7876
Toll Free: 1-888-233-4650
Participant Code: Redacted

International #'s (for Technical Bridge only):

Toll free	1-888-233-4650
Toll	1-719-234-7876
Local -Australia, Sydney:	+61 (0) 2 8207 3473
Local -Austria, Graz:	+43 (0) 316 218 875
Local -Austria, Vienna:	+43 (0) 1 274 872 5013
Local -Belgium, Brussels:	+32 (0) 2 300 1140
Local -Belgium, Liege:	+32 (0) 4 244 10 43
Local -Brazil, Sao Paulo:	+55 11 5582 6536
Local -Denmark, Copenhagen:	+45 70 14 49 50
Local -Finland, Helsinki:	+358 (0) 9 2311 4601
Local -France, Lille:	+33 (0) 359 30 21 52
Local -France, Lyon:	+33 (0) 426 23 61 04
Local -France, Marseille:	+33 (0) 488 56 43 01
Local -France, Paris:	+33 (0) 1 72 69 79 20
Local -Germany, Berlin:	+49 (0) 30 2555 5170
Local -Germany, Cologne:	+49 (0) 221 9688 180
Local -Germany, Frankfurt:	+49 (0) 69 12009 820
Local -Germany, Hamburg:	+49 (0) 40 2999 9160
Local -Germany, Munich:	+49 (0) 89 14367 050
Local -Hong Kong:	+852 3008 0316
Local -Ireland, Dublin:	+353 (0) 1 437 0811
Local -Italy, Milan:	+39 02 897 819 48
Local -Italy, Rome:	+39 06 452 170 39
Local -Italy, Turin:	+39 011 2179 2103
Local -Japan, Tokyo:	+81 (0) 3 4455 1487
Local -Netherlands,	+31 (0) 20 262 9505
Local -Netherlands,	+31 (0) 10 742 0133
Local -Norway, Oslo:	+47 21 54 70 76
Local -Scotland, Glasgow:	+44 (0) 141 404 9913
Local -Singapore:	+65 6517 0623
Local -Spain, Barcelona:	+34 93 802 0218
Local -Spain, Madrid:	+34 91 829 8566
Local -Spain, Valencia:	+34 96 314 6020
Local -Sweden, Stockholm:	+46 (0) 8 5205 4922
Local -Switzerland, Geneva:	+41 (0) 22 555 0201
Local -Switzerland, Zurich:	+41 (0) 44 556 8413
Local -UK, Birmingham:	+44 (0) 121 270 9912
Local -UK, Leeds:	+44 (0) 113 322 2683
Local -UK, Liverpool:	+44 (0) 151 203 9911
Local -UK, London:	+44 (0) 20 7078 9141
Local -UK, Manchester:	+44 (0) 161 241 9889
International toll free -	0800 666 3502
International toll free -	1 800 286 160
International toll free -Austria:	0800 293 304
International toll free -Belgium:	0 800 71 019

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000181

International toll free -Bulgaria:	00 800 115 1098
International toll free -Chile:	123 0020 9165
International toll free -China, Northern	10 800 714 1242
International toll free -China,	10 800 140 1236
International toll free -Colombia:	01 800 518 0884
International toll free -Czech	800 700 413
International toll free -Denmark:	80 889 327
International toll free -Dominican	1 888 751 4497
International toll free -Ecuador:	1 800 020 327
International toll free -France:	0 800 917 281
International toll free -Germany:	0 800 182 5931
International toll free -Greece:	00 800 161 2205 6755
International toll free -Hong Kong:	800 962 526
International toll free -Hungary:	06 800 164 94
International toll free -India:	000 800 1007 149
International toll free -Indonesia:	001 803 017 6755
International toll free -Ireland:	1 800 760 184
International toll free -Israel:	1 80 924 6079
International toll free -Italy:	800 871 134
International toll free -Japan:	00531 16 0894
International toll free -Latvia:	8000 2705
International toll free -Lithuania:	8 800 3 00 28
International toll free -Luxembourg:	800 2 8045
International toll free -Malaysia:	1 800 814 024
International toll free -Mexico:	001 800 514 6755
International toll free -Monaco:	800 93 466
International toll free -Netherlands:	0 800 022 8402
International toll free -New Zealand:	0 800 451 262
International toll free -Norway:	800 100 39
International toll free -Panama:	00 800 226 6755
International toll free -Poland:	00 800 112 40 22
International toll free -Portugal:	800 819 863
International toll free -Russia:	810 800 2749 1012
International toll free -Singapore:	800 101 2060
International toll free -Slovakia:	0800 606 260
International toll free -Slovenia:	0 800 80260
International toll free -South Africa:	0 800 981 302
International toll free -South Korea:	003 0813 2079
International toll free -Spain:	900 947 665
International toll free -Sweden:	02 079 9866
International toll free -Switzerland:	0 800 899 959
International toll free -Thailand:	001 800 156 205 6755
International toll free -Trinidad-	1 800 205 6755
International toll free -UK:	0 808 101 1679
International toll free -Uruguay:	0004 019 0245
International toll free -Venezuela:	0 800 100 8588

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000182

Appendix J – Physical Security Emergency Contacts

Name	Title	Work	Alternate	Cell
Sam Gregory	Contract Security Director - JWW	770.740.4751	Redacted	Redacted
April Mendez	Contract Security Site Manager- JWW	770.740.4244		
Quoizel Jackson	Contract Security Site Manager - 1550	404.885.8884		
Equifax 1550				
Front Lobby		404.885.8197		
Front Lobby Office		404.885.8234		
Security Booth		404.885.8883		
Loading Dock P-3		404.885.8430		
Equifax JWW				
Command Desk		770.740.5555		
Control Desk		770.740.4145		
Lobby One (Bldg 1505)		770.740.4741		
Lobby Two (Bldg 1525)		770.740.0880		
Lobby Two (waiting area)		770.740.6600		
Equifax NorthPark				
Security Desk (24hrs)	NorthparkAllied Barton	770.668.8020		
Lou Cray	Allied Barton Site Mgr. for Northpark	770.668.7909		Redacted
Emergency Officials				
Alpharetta Fire Dept.		**770.475.5900**		
Alpharetta Police Dept.		**678.297.6270**		
ATL Fire Dept.		**404.853.7072**		
ATL Police Dept.	**Zone 5**	**404.658.7054**		
Mid-Town Blue		**404.817.0500**		
Sandy Springs Police / Fire		**770.730.5600**		

Table J-1: List of physical security emergency contacts.

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000183

Appendix K – Payment Card Industry (PCI) and Contract Contact References

VISA
[HYPERLINK "http://usa.visa.com/merchants/risk_management/cisp_tools_faq.html" \h]
(Links titled "What To Do If Compromised" and "Responding To A Data Breach")
Visa Fraud Investigations and Incident Management group (650) 432-2978

MasterCard [HYPERLINK
"http://www.mastercard.com/us/merchant/security/sdp_program.h
tml" \h] (Link titled "MasterCard Data Security Rules (PDF)")
FRAUDULENT MASTERCARD E-MAIL OR SECURITY CONCERNS
please contact the
MasterCard Assistance Center:
Call collect from anywhere globally: +1-636-722-7111 or
toll-free from the United States: +1-800-627-8372 You may also send an e-mail to: [HYPERLINK
"mailto:consumer_advocate@mastercard.com" \h]

AMEX
[HYPERLINK
"https://www209.americanexpress.com/merchant/singlevoice/dsw/FrontServlet?request_type=dsw&pg_nm=merchinfo&ln=en&f
rm=US&tabbed=breach" \h]
[HYPERLINK
"https://www209.americanexpress.com/merchant/singlevoice/dsw/FrontServlet?request_type=dsw&pg_nm=merchinfo&ln=en&f
rm=US&tabbed=breach" \h]
Please see the AMEX Data Security Operating Policy Section 2, for all details pertaining to Data
Incident Management Obligations.
American Express Enterprise Incident Response Program (EIRP) toll free at (888)732-3750/US only, or
at 1(602)537-3021/International or email [HYPERLINK "mailto:EIRP@aexp.com" \h]

DISCOVER
[HYPERLINK
"http://www.discovernetwork.com/fraudsecurity/databreach.html"
\h] Discover Network Incident Response Team
Merchants: (800) 347-3083
Acquirers (800) 347-7052

JCB
[HYPERLINK "http://www.jcbusa.com/" \h]
Tel:1-800-736-8111(Toll Free)
or 212-651-8011

For all Client Incident notifications, the Cyber Threat Center will work with corporate communications, and through the Client relationship managers to appropriately contact any clients that are affected by an incident, in the agreed upon manner for each client. The Equifax "COE OPS-IT Champions" distribution list shall be used to contact the most appropriate POC, when a more specific manager is not known.

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000184

Acknowledgements

This document was derived in conjunction with NIST Special Publication 800-61, Computer Security Incident Handling Guide. Special Publication 800-61 it based on ITL's research, guidance, and outreach efforts in computer security and its collaborative activities with industry, government and academic organizations. SP 800-61 is often considered as best practices by security personnel. SP 800-61 should be used as a reference guide in conjunction with this document.

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC. EFXCONG-SBC000000185