

**Statement of Maria T. Vullo, Superintendent
New York State Department of Financial Services
Testimony to the New York State Senate Standing Committee
On Consumer Protection -- Identity Theft**

September 28, 2017

Good morning. Thank you, Chairman Carlucci, Ranking Member Comrie and members of the Senate Standing Committee on Consumer Protection, for the opportunity to provide testimony regarding the growing problem of identity theft. I commend the Committee for examining this issue and for seeking ways to combat this insidious threat. As the Superintendent of Financial Services, I can tell you that my agency, the Department of Financial Services (DFS), and the Governor's administration, takes this issue extremely seriously and that we are doing whatever we can to protect New York consumers and markets in this challenging time.

As both a regulator and an enforcement agency, DFS plays a unique and key role in protecting consumers against identity theft. And with the federal government increasingly renegeing on its obligations to consumers, strong state regulation and oversight are necessary to

safeguard the private information that is provided to the financial institutions and companies that provide financial services and products to New Yorkers who rely on these companies to keep their personal information safe from hackers and cybercriminals. The Equifax data breach is a wake-up call on this very issue.

Since its creation in 2011, DFS has been keenly focused on combatting identity theft and educating consumers on ways to avoid it. DFS provides consumer information about how they can clear their name, and we make sure that our financial institutions resolve customer complaints promptly and effectively. We see many types of complaints in this area. Some are fairly straightforward, like when an identity thief uses stolen information to siphon cash directly out of a victim's bank account. Others are more complicated, involving running up thousands of dollars in debt through fake credit cards linked to victims who have no idea what happened until they are contacted by aggressive debt collectors. In all of these cases, DFS works tirelessly to assist

consumers and ensure that financial institutions are responding and resolving issues appropriately.

To keep the public vigilant and educate them about this growing problem, DFS also conducts community outreach on identity theft. Our consumer representatives partner with local organizations in communities across the state to educate consumers about identity theft, and provide ways for people to protect themselves. We have developed a brochure about the issue, which is distributed throughout the state, and is included on our website. Through our Consumer Hotline — (800) 342-3736 — consumers can get information about identity theft, and they can file a complaint through an online DFS portal if they believe they have been a victim of identity theft.

Unfortunately, as the recent Equifax breach so clearly demonstrated, no one is safe from identity theft. Not the old, not the young – not even children. Identity theft affects *all* of us. And the impact can be financially and emotionally devastating. It can result in damaged credit, denial of employment, loans and other credit, denial of

professional licenses, and can even impact a victim's medical treatment. It can take years for someone to recover from identity theft. Young people applying for credit for the first time, perhaps for a college loan or a credit card, can be shocked to discover that their identity has been stolen and their credit ruined. Potential homebuyers applying for a mortgage have had to put their dreams on hold when they found out their private information had been compromised.

We recommend that all consumers, regardless whether they think they may be victims of identity theft, check their credit reports for signs of identity theft regularly, and monitor their credit cards, monthly bills and bank statements on a regular basis. We further recommend that consumers who think they may be a victim of identity theft consider placing a credit alert or security freeze in their files; we suggest that identity theft victims file a police report and Identity Theft Affidavit; and we caution consumers and especially security breach victims to be wary of pretexting calls, phishing scams, and attempts to profit from the breach. Our brochures on identity theft and security breaches contain

details and suggestions for consumers seeking to protect themselves from identity theft.

The Equifax hack has put this issue front and center for millions of Americans – and New Yorkers – who are now looking for information and guidance in the wake of this enormous cyber breach.

Equifax — which has data on nearly 1 billion people and 100 million companies — recently announced that hackers had infiltrated its systems sometime between mid-May and July. According to Equifax, 143 million Americans (about 8 million New Yorkers) had their names, birthdates, Social Security numbers, driver’s license numbers, credit card numbers, and dispute documents containing personal information released. Every one of these 143 million people whose information was breached is now at a heightened risk of identity theft. That’s 44% of the population of the United States. Much is still unknown about the breach and the situation is unfolding daily. It is very concerning to me and my staff, and we are working night and day on several fronts to address this situation for New Yorkers.

While the Equifax issue has certainly shined a much needed spotlight on the real danger consumers and our financial institutions face, I have been sounding the alarm about cybersecurity – and taking decisive action – since I arrived at DFS over 19 months ago. Given the amount of personal data received and kept by the financial services industry, it is vitally important that those institutions adopt cybersecurity programs to protect that data. This is why DFS acted last year to propose – and this year to finalize – a first in the nation cybersecurity regulation that requires cybersecurity minimum requirements for financial institutions regulated by DFS. This should be a no brainer, but no other federal or state regulator has acted with a regulation like the one that DFS proposed in September 2016 and adopted in March 2017. Our financial system is at constant risk from cybersecurity threats, both foreign and domestic, internal and external. Our regulation therefore requires that the financial institutions develop proactive and constantly evolving cybersecurity programs to stay ahead of cyber threats. Institutions that we trust with our personal data must understand the importance of that trust, take seriously their obligations to protect our

data, and be aware that they will pay a stiff penalty if they fail to utilize sufficient cybersecurity protections.

After becoming aware of the Equifax breach, DFS acted quickly with actions to address the problem in New York. We issued alerts to our financial institutions and to New York consumers. Our Consumer Alert provided background on the breach, advised consumers of the actions they may take to protect themselves, and alerted consumers to scams that could stem from the breach that they should take caution to avoid. DFS also issued guidance to all New York State-chartered and licensed financial institutions, both banks and insurance companies, urging them to take immediate action and undertake precautions to protect consumers, including making sure that the institutions we regulate take steps to:

- Install security patches for their systems;
- Adopt and follow ID theft and fraud prevention programs for customer due diligence/Know Your Customer confirming information from Equifax before relying on it;

- Consider a customer call center for customers to call if their information has been hacked, and, in such cases, consider coding the customer account with a “red flag” to contact the customer at a pre-designated contact number or e-mail address prior to opening an account, issuing a credit card, providing a loan or making any changes to existing accounts; and
- Review the terms of their arrangements with Equifax to determine any potential risk if the institution continues to provide account and debt information to Equifax.

DFS also responded to the Equifax incident by promulgating a new regulation requiring credit reporting agencies to register with DFS and follow important consumer protections, including DFS’s first-in-the-nation cybersecurity regulation. Under this new regulation, every credit reporting agency will be required to comply with DFS’s landmark cybersecurity regulation, which was finalized this year and already applies to all banks, insurance companies and other financial institutions regulated by DFS.

This proposed regulation, which is subject to a 45-day comment period, subjects credit reporting agencies to examinations by DFS as often as the Superintendent determines is necessary, and prohibits credit reporting agencies from, among other things:

- Directly or indirectly defrauding or misleading a consumer;
- Engaging in any unfair, deceptive or predatory act toward any consumer;
- Misrepresenting, omitting facts or including any inaccurate information in the assembly, evaluation, or maintenance of a credit report for a New York consumer; and
- Refusing to communicate with an authorized representative of a consumer located in New York State who provides a written authorization signed by the consumer.

Furthermore, under this regulation, the Superintendent of Financial Services has the authority to deny and potentially revoke a consumer credit reporting agency's authorization to do business in New York if the company is found to be out of compliance with certain prohibited

practices, including those just mentioned and DFS's cybersecurity regulation.

All credit reporting agencies, like all regulated financial services institutions doing business in New York, will be required to develop a comprehensive risk-based cybersecurity program, to have adequate controls in place to protect their information systems, to report a known cyber breach within 72 hours, to utilize vulnerability scans, penetration testing and encryption to protect customer private data, and to have a responsible Chief Information Security Officer reporting to the Board of Directors on the company's cybersecurity program. It simply is unacceptable for a company that profits from consumers' private information to fail to have adequate protections. As I said, the facts about what happened at Equifax are still unfolding, and DFS is investigating this matter thoroughly on behalf of the people of this State.

Strong regulation is critical to combatting problems like identity theft. Regulators like DFS can go beyond after-the-fact law enforcement actions to prevent further harm and act quickly to contain any damage.

New York's regulated financial services firms are now beefing up their cybersecurity programs and practices because of the DFS regulation. I am working through the National Association of Insurance Commissioners so that they adopt a model law consistently with the DFS regulation for all insurance companies. I am working hard to implore federal banking agencies to do the same. We cannot afford to talk about it anymore – we must act on it. I can assure you that DFS will continue to act when and where we can to protect our markets and consumers in New York. And DFS will utilize the full breadth of its powers to address the Equifax breach and take proactive steps to reduce the likelihood of something like this happening again.

I commend you for taking steps as legislators to address this serious issue. I understand that several bills have been proposed to address the serious breach experienced by Equifax and the regulatory framework for credit reporting agencies. Credit reporting agencies are a critical spoke in the wheel that constitutes our financial services industry. Virtually every financial institution shares information with

and relies upon information from credit reporting agencies. As I have described, DFS already has taken several regulatory actions to fill the void in federal regulation in this area. State legislation to require that credit reporting agencies provide New York consumers with further protections and that require such agencies to be licensed by DFS are important efforts to ensure that these companies are properly supervised and held accountable. In this regard, I cannot stress enough the importance that any legislation include teeth in the form of stringent penalties available at my disposal as DFS Superintendent to enforce the requirements of the law. As the regulator of New York's financial services industry as well as a law enforcement agency, DFS is uniquely positioned to address these matters in a holistic manner.

In closing, the data breach at Equifax demonstrates the necessity of strong state regulation, as we have recently promulgated at the Department of Financial Services, combined with consumer education and outreach, to keep our regulated institutions and consumers safe from cybercriminals and identity thieves. DFS will continue to take strong

actions to safeguard New York's markets and consumers, and will hold responsible those who breach New Yorkers' sensitive information. As always, I am happy to work with all of you to protect New Yorkers through effective laws.

Thank you.

###

Testimony

New York State Senate Consumer Protection Committee Hearing on Identity Theft

September 28, 2017

The Office of the New York State Attorney General

Clark Russell

Deputy Bureau Chief

Bureau of Internet and Technology

Good morning Chair Carlucci, Ranking Member Comrie and distinguished members of the Senate Consumer Protection Committee. My name is Clark Russell and I am the Deputy Bureau Chief of the Bureau of Internet and Technology at the New York State Attorney General's office. The Bureau of Internet and Technology is responsible for protecting consumers and families from existing as well as new and developing online threats. Thank you for the opportunity to provide testimony regarding the challenges we are facing protecting consumers from identity theft.

The Equifax data breach is an unprecedented event. More than 140 million Americans, which is more than half of the adults in this country, including over 8 million New Yorkers, had their most sensitive personal information stolen, placing them all at risk of identity theft and hindering their ability to buy a home, start a business, or get a job. Although I cannot discuss any details today, our office has opened an investigation into exactly what happened. And from the moment we learned of the breach, we have been pressing Equifax on a number of issues -- including a delay in notifying consumers of the breach; a forced arbitration clause in their free credit monitoring contracts that they've since removed and their failure to provide Spanish-language customer service to consumers affected by the breach. Following conversations with our office, Equifax has addressed all of those issues and has just agreed to provide consumers the ability to lock and unlock their credit file for life. We have also raised data security questions with the two other major credit bureaus: TransUnion and Experian. We will use all of the tools at our disposal to get to the bottom of the Equifax breach, and ensure that all three credit bureaus take effective steps to protect the sensitive information they possess.

While the Equifax breach is unique in the scale and severity of the information theft, in many ways it is merely an escalation of a disturbing trend that the Attorney General's Bureau of Internet and Technology has observed over the past several years. Under General Business Law § 899-aa, companies are required to notify consumers and our office of a data breach. As we addressed in a report issued earlier this year, in 2016 the office received 1,300 data breach notices – up 60% from the year before. The main causes of data breaches are hacking, which accounted for 40% of reported data security breaches in 2016, and employee negligence, which accounted for 37% of reported breaches. In recent years, we have received data breach notifications from Home Depot, reporting 56 million credit card numbers disclosed; Target, reporting 40 million credit card numbers disclosed; and Anthem, reporting over 78 million records disclosed including social security numbers.

Unfortunately, when a breach occurs, consumers often have limited options. Credit monitoring helps consumers identify suspicious transactions, but it only alerts the consumer after someone has already stolen her identity. Credit freezes stop wrongdoers from opening a line of credit in a consumer's name, but a thief can still file for government benefits in the consumer's name or file a fraudulent tax return.

We all need to do more. Businesses should only collect the information they need to conduct their business, and securely delete and destroy it when it is no longer needed. They should design and implement an information security plan. They should designate a person responsible for the plan and educate and train their employees. Finally, they should continually review their plan and revise it as new threats emerge or their business changes.

Consumers need to stay vigilant. They should create strong passwords for online accounts, and use different passwords for different accounts. They should carefully monitor credit card statements and contact their bank immediately if they see a suspicious transaction. In addition, to avoid computer viruses and online scams, they should avoid opening suspicious email or clicking on suspicious hyperlinks.

The Legislature has an important role to play in protecting consumers from threats as well. New York's data security laws are in dire need of updating. That is why, for several years, Attorney General Schneiderman has been pushing for a major overhaul of New York's data security law. At a minimum, the law must be updated to require companies to have "reasonable" security measures, modernize the definition of "private information," and provide a safe harbor for companies that adopt model data security. I will discuss each of these components in more detail.

The law should require that all entities that collect or store private information have "reasonable" security measures. It may be surprising to learn that there is no statutory law requiring a company to maintain "reasonable data security," except if it collects Social Security Numbers, or if the company is in health care or the financial industry and governed by a specific regulatory framework. The law only requires that a company provide notice to consumers and the New York Attorney General's office if there is a breach of "private information," which is generally defined as a person's name in combination with a Social Security number, driver's license, or account or credit card number.

The "reasonable" standard is a common legal standard that would take into account the size of the company, the type of information it keeps, and other facts in deciding whether the entity had acted reasonably. A mom-and-pop grocery store should have far different "reasonable" security measures than a multinational credit reporting agency, for instance. For a small business or one that does not collect sensitive personal information, reasonable security measures might only mean purchasing an antivirus program. For larger businesses or those that collect personal information, reasonable security measures might include physical safeguards, such as locks to protect physical areas where information is stored, as well as administrative safeguards, such as assigning responsibility for data security to a particular employee.

In addition, the definition of "private information" in existing law needs to be modernized. For example, it might be shocking to learn that if you maintain a Google Gmail account, and Google gets hacked resulting in the theft of your user name and password, Google is not statutorily required to tell you. If a biometric authenticator, such as a fingerprint or a facial scan used to unlock an iPhone, is disclosed to a hacker, Apple is not statutorily required to tell you. This needs to change.

Finally, while the law needs to be updated to protect consumers, we also need to make sure that the law does not unduly burden companies. The law should provide a safe harbor to companies already subject to federal or other New York State data security regulations, and in compliance with those rules, so they will not need to worry about overlapping or conflicting regulations. Similarly, companies that are certified for complying with leading industry data security guidelines should be presumed to have reasonable data security.

Thank you. I am happy to answer your questions.

Senate Standing Committee on Consumer Protection
Hearing On How Best To Protect Consumers from the Theft of Their Personal
Information

Thursday, September 28, 2017

The New York Credit Union Association

Testimony by Henry Meier, General Counsel

Chairman Carlucci

Ranking Member Comrie

Good Afternoon,

My name is Henry Meier. I am the General Counsel of the New York Credit Union Association, which represents more than 80 percent of both federal- and state-chartered credit unions in New York State. For 100 years, the Association has been dedicated to making sure that the member-owners of the state's credit unions have access to cost effective financial products and services. Because credit unions are, by definition, member-focused, consumer protection has always been one of their primary goals.

The Association appreciates the opportunity to testify at today's timely hearing. Because of our hands-on approach to banking, we are uniquely positioned to identify the needs of consumers and to offer solutions to the growing problem of data breaches and related identity theft.

Not too long ago, it was common for member information to be stored in the house of the CEO or for loan payments to be personally collected by board members. Times change. While technology enables credit unions to connect with their members in ways that would have been unimaginable just a generation ago, this same technology also makes it easier to steal member information.

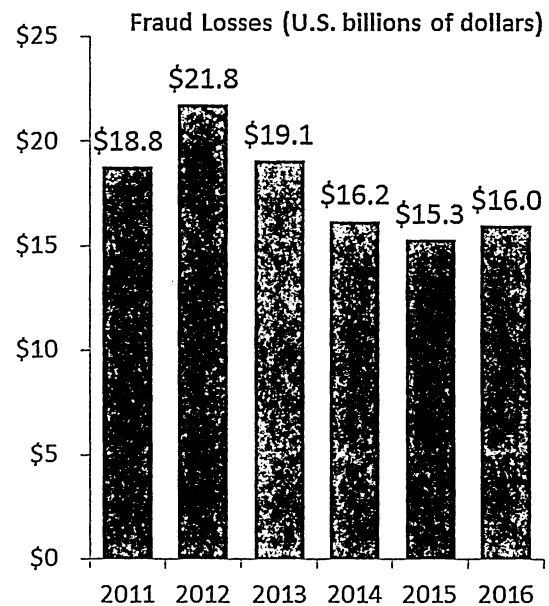
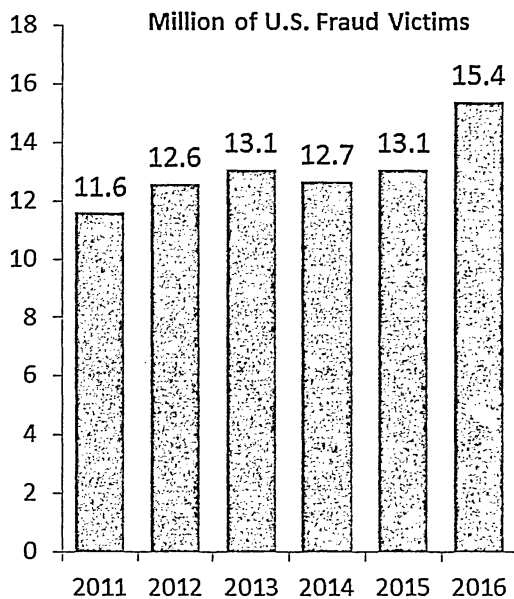
The Equifax data breach is a wakeup call for policymakers, businesses and consumers that more needs to be done to protect personal information. Identity theft rose sixteen percent in 2016, impacting more than 15 million Americans and costing \$16 billion in losses¹. There are no legislative silver bullets that can make the problem go away; a fact of life made much more dangerous and far reaching by the internet.

The good news is that there are steps that legislators can take to better protect consumers from identity theft. These steps include:

- Imposing baseline data security protections not just on financial institutions but on any industry that holds a large amount of personally identifiable consumer information;
- Fostering a greater commitment to the robust protection of consumer information by imposing liability on all businesses that negligently store consumer information;
- Educating consumers to be more active in monitoring and protecting their personally identifiable information; and
- Avoiding duplicative requirements that don't enhance consumer safety but make protecting consumers more expensive.

¹ See: <https://www.javelinstrategy.com/press-release/identity-fraud-hits-record-high-154-million-us-victims-2016-16-percent-according-new>).

Total Fraud Victims Reaches Record High



Source: 2017 Identity Fraud Study, Javelin Strategy & Research.

JAVELIN

Credit Unions Are Already Subject To Extensive Identity Theft Prevention Requirements

Credit unions are already subject to extensive cybersecurity regulations and requirements that guard against identity theft. At the federal level, the Consumer Financial Protection Bureau (“CFPB”), Securities and Exchange Commission (“SEC”), Federal Reserve System (“Fed”), Federal Trade Commission (“FTC”), and the National Credit Union Administration (“NCUA”) provide cybersecurity regulations, requirements and guidance to the financial services industry. These comprehensive requirements govern all areas of cybersecurity protection, including board engagement, staffing and management, written information security plans, cybersecurity training, technical controls, disposal of sensitive information, and numerous other aspects of cybersecurity².

In fact, for more than a decade, both state and federal credit unions have had to conduct risk assessments to identify accounts that pose a reasonably foreseeable risk of identity theft, taking into consideration the methods used to open and access accounts, and the institution’s previous experiences with identity theft.³

² See: FFIEC Cybersecurity Assessment Tool, available at: https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_May_2017.pdf.

³ See: Section 12 CFR 717.90, available at <https://www.law.cornell.edu/cfr/text/12/part-717/subpart-J>.

This means that there are persons at every credit union whose responsibilities include monitoring account activity for signs that members are being victimized by identity theft and staying informed about the latest cyber-developments to assess how they might impact credit union operations.

This framework is not foolproof. But by already having a mandatory framework in place for identifying and evaluating identify theft threats on an ongoing basis, credit unions and other similar depository institutions have something to follow.

In contrast to credit unions, retailers are under no corresponding requirement. This is true even though large retailers such as Target and Walmart have access to more consumer information than the largest banks. Equifax is not yet subject to New York's new cybersecurity regulations even though all but the smallest state-chartered credit unions have already been working towards complying with this mandate.

Against this backdrop, both regulators and legislators have to level the playing field with regard to the protection of consumer information. It simply makes no sense that large businesses that utilize and store consumer information face fewer requirements to protect consumer information than do even the smallest credit unions.

It is crucial, however, that as legislators and regulators examine ways to make more businesses responsible for protecting consumers, they remain mindful of the obligations that are already imposed on credit unions and financial institutions. There is simply no need to duplicate federal mandates.

What Happened At Equifax Is All Too Common

The Equifax data breach is noteworthy for its size, but in reality, what happened is an all-too-common occurrence in which companies use inadequate security standards, while consumers and financial institutions pay the price.

The scenario goes something like this: a company finds out that hackers have been able to steal troves of personal information. As the company investigates the break-in, it finds out that the compromise was facilitated by an oversight in its security procedures such as failing to promptly install the latest software update. It informs law enforcement of the hack but waits several weeks before telling consumers that their information has been compromised.

When consumers get the news, they understandably reach out to their credit union and often request that their debit and credit cards be replaced.

As a result, credit unions and banks must absorb a disproportionate share of the costs associated with the breach of consumer information. One leading study concluded that data breaches cost companies \$225 for each compromised record. That same study reported that the costs of compromised records is \$100 greater for financial institutions⁴.

⁴ See: 2017 Cost of Data Breach Study: United States, available at <https://public.dhe.ibm.com/common/ssi/ecm/se/en/sel03130usen/security-ibm-security-services-se-research-report-sel03130usen-20170825.pdf>).

When Home Depot was hacked, credit unions spent \$60 million reissuing cards and covering costs associated with the breach.⁵

In addition to the direct financial costs, there are indirect costs that are harder to quantify but have a very real impact on credit union operations. For example, even though credit unions are not responsible for the vast majority of data breaches, they run the risk of being associated with the misconduct of other companies over which they have no control. After all, a credit union member who hears of a breach, turns to the credit union for answers and not the company responsible for the mishap.

Existing Legal Remedies Do Not Adequately Compensate Members Or Credit Unions Against Loss

Given the costs and reputational risks posed by data breaches, existing legal remedies do not go far enough in holding companies that negligently safeguard consumer information accountable.

In Spokeo, Inc. v. Robins, 136 S.Ct. 1540, 2016, the Supreme Court held that in order to establish Article III standing, a plaintiff must show that he or she has suffered “an invasion of a legally protected interest” that is “concrete and particularized” and “actual or imminent, not conjectural or hypothetical.”

Courts have had difficulty applying this standard to cases in which consumer information has been compromised. For example, at least one circuit court has refused to allow consumers to sue a grocery store chain that they contend did not adequately protect their personal information because the consumers could not prove that their compromised information was used to facilitate a data breach.⁶

The result of these legal hurdles has been that the proportion of federal data breach lawsuits actually declined last year.⁷

The Legislature should give both businesses and consumers that have been victimized by data theft the right to sue so long as they can prove their personal information has been compromised. No one should have to wait for their private information to be used against them before forcing the companies responsible for compromising their information to take appropriate action.

Minnesota demonstrates how this approach would work. The Plastic Card Security Act allows financial institutions to sue entities that negligently store and retain credit and debit card information longer than is necessary. The bill allows injured businesses to sue for the cost of replacing debit and credit cards.⁸

The utility of this legislation to aid consumers was underscored in litigation following the Target data breach. When the company argued that a class action lawsuit brought against it should be dismissed, the Federal District Court overseeing the case refused to do so, pointing out that “while courts are reluctant to recognize duties of care in the absence of legislative imprimatur, the duty to safeguard credit- and debit-card data in Minnesota has received that legislative endorsement.”⁹

⁵ See: BankInfoSecurity October 30, 2014, available at <https://www.bankinfosecurity.com/home-depot-breach-cost-cus-60-million-a-7504>

⁶ See *In re SuperValu, Inc.*, No. 16-2378, 2017 WL 3722455, at *1 (8th Cir. Aug. 30, 2017).

⁷ See: “Bryan Cave’s 2017 Data Breach Litigation Report” available at <https://d11m3yrngt251b.cloudfront.net/images/content/9/6/v2/96690/Bryan-Cave-Data-Breach-Litigation-Report-2017-edition.pdf>.

⁸ See: section [325E.61](#), Minnesota Statutes Available at <https://www.revisor.mn.gov/statutes/?id=325E.64>

⁹ See: *In re Target Corp. Customer Data Sec. Breach Litig.*, 64 F. Supp. 3d 1304, 1310 (D. Minn. 2014).

Passage of similar legislation in New York would signal that the Legislature is committed to letting consumers have their day in court.

Technology Can Help Prevent Identity Theft

There is an assumption that technology and consumer protection will always conflict. But the experience of some of our credit unions demonstrates that this does not have to be the case.

The mortgage lending process has traditionally been labor intensive. To do mortgage lending, credit unions must employ loan originators who deal with mortgage applicants, underwriters who assess an applicant's eligibility, staff who fill out the ever-increasing number of forms, servicers who ensure that payments are made, and of course lawyers to make sure all this is done consistent with the law.

However, thanks to technology, it is now possible for even small credit unions to utilize software that does many of these tasks quickly and efficiently. For example, much underwriting is done with the help of computer algorithms as software can be used not only to generate the appropriate paperwork, but to make sure that a member receives these disclosures in a timely fashion.

What's important to keep in mind for the purpose of this hearing, is that the same technology can cut down on the opportunities that hackers have to engage in data theft. For example, instead of asking a member to email paystubs to an originator, a member can be directed to a secure database where he or she can directly and safely input the necessary information. The end result is a more efficient, quicker mortgage process that more adequately protects member information.

Consumer Education Must Also Play A Role

For any framework designed to reduce identity theft to be truly effective, consumers must be active participants and not simply passive observers when it comes to protecting their financial information.

Some of the steps they can take are now well known. For example, they need to be cognizant of the fact that any time they put information on Facebook or other social media, they are potentially more vulnerable to hackers. After all, innocent facts such as the name of their dog or that their mother is celebrating her birthday can provide key information to persons looking to steal identities.

Interestingly, even consumers with little or no online presence are at risk. Typically, they take up to 40 days longer to notice and report security breaches, and on average suffer larger losses.¹⁰

More generally, the Association believes that the more consumer savvy a member is, the better able they will be to prevent identify theft and minimize its consequences if it occurs. This is one of the reasons why in the coming months we will be reaching out to the education community and advocating for the introduction of more consumer education in our elementary school through high school curriculum. If we've learned anything from the financial crisis of 2008, it is that members need to know how to protect themselves, and that starts with understanding how the banking system works.

While there is much that the State can and should do to protect consumer information, ultimately this is a national problem that demands a national solution. On the federal level, the Credit Union National

¹⁰ See: <https://www.javelinstrategy.com/press-release/identity-fraud-hits-record-high-154-million-us-victims-2016-16-percent-according-new>).

Association has joined with its National Trade Organizations in advocating for the imposition of baseline cybersecurity requirements for all industries. The internet does not respect state and national borders.

But, we don't have time to wait for federal action. The Equifax data breach has underscored just how vulnerable consumers are to identity theft. There is much that can and should be done to protect New Yorkers right now.

Thank you.

STATE PRIVACY AND SECURITY COALITION



September 28, 2017

The Honorable David Carlucci, Chairman
Senate Consumer Protection Committee
Albany, NY

Re: How Best to Protect Consumers from Theft of their Personal Information

Dear Chairman Carlucci,

The undersigned associations represent thousands of the country's leading technology companies in high-tech manufacturing, computer networking, information technology, clean energy, life sciences, Internet media, ecommerce, education, and sharing economy sectors. Our member companies are committed to advancing public policies and private sector initiatives that make the U.S. the most innovative country in the world. We share your concern about the security of sensitive consumer personal information; in fact, our members invest hundreds of millions of dollars each year to protect this information. Many also provide consumers with services, such as security software and secure storage solutions, to help consumers protect their own information.

Existing standards, such as those issued by the International Organization for Standardization (ISO) and the Cybersecurity Framework developed by the Department of Commerce's National Institute of Standards and Technology (NIST), address the protection of consumer personal information. In addition, both existing federal and New York State laws provide strong protections. New York law includes a strong data breach notification law enforced by the New York Attorney General. The New York Department of Financial Services also promulgated extensive security regulations this year that apply to a wide range of entities subject to the State's Banking, Insurance, and Financial Services laws. The Federal Trade Commission has a robust enforcement program relating to data security. In addition, other laws impose significant sectoral security obligations, such as the HIPAA and CPNI security requirements that apply to consumer data held by many New York companies.

Regulation is not a silver bullet in the protection of personal data. There is tremendous innovation in attack methods, much of it driven by nation states deploying new cyber weapons that are then copied by criminal hackers. Attack techniques have penetrated the systems of the

State Privacy & Security Coalition, LLC
500 8th Street, NW
Washington, DC 20004
202.799.4000 Tel

National Security Agency, the CIA, and the Department of Defense. Expecting private companies to withstand these sorts of attacks in all cases is not realistic. What is more, because attack methods continue to adapt and evolve, data security invariably has to adapt and evolve, as well.

Rather than a compliance-based, “screenshot-in-time” approach, the challenging task of data security instead requires a flexible, risk-management approach that identifies and responds quickly to changing attack methods and recognizes that these attack methods will inevitably result in cyber intrusions. The NIST Cybersecurity Framework developed through a partnership of the Obama Administration and the private sector sets forth best practices and standards to provide guidance that is helpful at driving better security. Implementation varies based upon the context and size of the specific organization using the Framework.

With regard to data security specifically, the Federal Trade Commission has laid out important principles in its “Start with Security” Guide, which sets out a list of the types of measures (not a checklist) which, in combination, the FTC recommends that businesses use to help secure sensitive consumer information. Best practices can and will change in the future, as threats and security techniques evolve.

Other policy ideas, though, would undermine rather than advance data security. One idea that has surfaced recently is a 15 day quick breach notice to individuals whose private information was, or is reasonably believed to have been, acquired by a person without valid authorization. No state has adopted any deadline of such short magnitude, most notably because it is well known and understood that breach investigations of hacking incidents often take substantially longer than 15 days to identify the nature and scope of a breach, who was affected by a breach, and whom to notify. In the immediate aftermath of a data breach incident, companies should focus their time and resources on investigating and containing the breach, and securing the company’s systems. Imposing an unrealistically short notice deadline would divert companies’ resources away from these critical, time-sensitive tasks by injecting a compliance obligation to identify individuals affected before taking these other important steps. It would greatly increase the risk of inaccurate and premature notice that either over or understates the scope of a breach, thereby causing confusion. Most importantly, it would divert company resources and cause delay to essential remediation activities without providing any additional, meaningful safeguards for consumers.

Personally Identifiable Information as it pertains to Internet Service Providers

We also understand you have interest in the issue of the protection of personally identifiable information as it pertains to Internet Service Providers (ISPs). Twenty-eight states have already considered and rejected legislation on this issue for very good reason; our members oppose legislation on this matter, as well. ISP privacy legislation by an individual state jurisdiction is unnecessary because this issue is already well addressed by existing federal and state laws.

ISP customers are already protected from having data such as their personal web browsing history sold without consent. All major ISPs have designed their privacy practices

based on the FTC's privacy framework, which includes guidance on transparency and choice. ISPs also committed in January of this year to adhere to ISP Privacy Principles, which are consistent with the FTC privacy framework. Moreover, a number of ISPs have publicly noted that they do not sell their customers' personal web browsing histories and most have privacy policies that would prevent such behavior. The FTC and many state attorneys general across the country have powerful tools to hold ISPs accountable for breaking these promises.

Because broadband service is critical to e-commerce, creating new and different standards in New York could lead to unintended consequences for consumers and businesses. ISPs would be forced to adjust their investment and technology deployment plans based on a singular set of rules for the State. Legislation in this area risks stifling investment and innovation by existing ISP providers and new entrants, both of whom could be restricted from, for example, developing new and innovative ways of making the Internet, content, and online services accessible to consumers.

Arguments that the Congressional action preventing the FCC broadband privacy rules from taking effect has reduced privacy protections for consumers are simply false. As explained above, a variety of state and federal laws continue to provide robust protection for consumers' personal information.

The Existing Privacy Regulatory Framework Already Protects Consumers

On May 18th, the FCC voted to begin a process that would ultimately result in broadband services no longer being classified as a Title II service. Acting FTC Chairman Maureen Ohlhausen lauded this decision as the first step in restoring FTC oversight of ISP consumer privacy. Even before that restoration occurs, the privacy practices of ISPs are already subject to several layers of regulatory and other enforceable restrictions.

- **Section 222 of Communications Act**

The FCC has made clear that it applies Section 222 of the Communications Act to ISPs. Section 222 imposes a duty of confidentiality on carriers, which continue to apply to broadband ISPs as they are currently classified as Title II services.

In 2015 the FCC issued an enforcement advisory advising broadband ISPs how the Commission intends to enforce Section 222 against such providers, stating: "By examining whether a broadband provider's acts or practices are reasonable and whether such a provider is acting in good faith to comply with Section 222, the Enforcement Bureau intends that broadband providers should employ effective privacy protections in line with their privacy policies and core tenets of basic privacy protections." Earlier this summer, in an order adopted on June 26, 2017, current FCC Chairman, Ajit Pai, reiterated this enforcement advisory and reminded ISPs that they "remain subject to Section 222."¹

¹ http://transition.fcc.gov/Daily_Releases/Daily_Business/2017/db0629/FCC-17-82A1.pdf

and Washington, as well as in western states such as Nevada and Montana. There is increasing concern and recognition of the unintended consequences and negative repercussions that could result from legislation of this kind.

For these reasons, our members oppose legislation imposing privacy requirements on ISPs.

In summary, we urge this Committee to recognize the complexity of data security, the need for flexibility in a rapidly evolving space, and the strong laws already in place to encourage good data security practices.

We hope that this letter is helpful to your Committee and would be happy to answer any questions you may have.

Sincerely,

State Privacy & Security Coalition
Association of National Advertisers (ANA)
CompTIA
TechNet



**STATEMENT OF THE
NEW YORK PUBLIC INTEREST RESEARCH GROUP (NYPIRG)
BEFORE THE NEW YORK STATE SENATE
COMMITTEE ON CONSUMER PROTECTION
REGARDING IDENTITY THEFT
SEPTEMBER 28, 2017
ALBANY, NEW YORK**

Greetings. My name is Russ Haven and I am General Counsel of the New York Public Interest Research Group (NYPIRG). NYPIRG appreciates this opportunity to discuss the most recent data security breach, the problem of identity theft and ways to protect consumers.

This hearing occurs in a world where our digital footprints are tracked virtually every moment of the day, where our most sensitive personal and financial information can be captured without our knowledge and then hijacked by sophisticated crime operations, draining the economy and creating havoc in our lives. Many Americans feel a profound sense of unease over “data insecurity.”

Along with other consumer advocacy groups, NYPIRG has long criticized consumer data surveillance firms, also known as credit reporting agencies, particularly the “Big Three” credit bureaus that have data files on virtually every American: TransUnion, Experian and Equifax.¹

In the past our criticisms have focused on credit reporting errors and failures to correct problems. Recent events indicate that credit bureaus—which have staked their reputations on securely storing confidential consumer information—may be doing a poor job in this essential function.

¹ Many other firms sell credit reports, but the three national credit bureaus are the ones relied on primarily by lenders. Other data firms have a particular market niche, ChekSystems, for example, reports on checking account activity rather than credit-handling experience.

Most obviously, Equifax's announcement that information, including names, dates of birth, social security numbers and drivers' license numbers for 143 million consumers, 182,00 files of consumers with disputes in progress, and more than 200,000 credit card numbers have been hacked through a weakness in the company's website. This has appropriately sent shock waves through the American public and sent consumers scrambling for information on credit freezes and fraud alerts.² This staggering breach affects half of all U.S. residents and some eight million (8,000,000) New Yorkers.³

Adding insult to injury, reportedly three top Equifax staff unloaded stock in the company worth \$1.8 million after Equifax learned of the breach but *before* regulators and the public were notified. The U.S. Department of Justice and the Securities and Exchange Commission are said to have opened an investigation on what may have been insider trading.⁴

The Experian data breach was the largest ever recorded involving social security numbers, a key piece of information for identity thieves, according to the Identity Theft Resource Center, a nonprofit organization that assists victims of identity theft.⁵

Identity Theft

Consumers worry about the security of their personal and financial data held by others for good reason: Identity theft remains a top consumer problem.⁶ Identity theft can cause major disruptions for consumers, even when victims are relieved of footing the bills racked up by thieves, their time and out-of-pocket expenses and stress all take a toll. In extreme cases, problems can hound consumers for years, making it difficult to obtain and constantly defending against bills run up by a thief from long ago.

Identity theft continues to be among the top three consumer complaints received by the Federal Trade Commission. For 2015, the last year for which data were evaluated,

² *Equifax Says Cyberattack May Have Affected 143 Million in the U.S.*, Tara Siegel Bernard, Nichole Perlroth, and Ron Lieber, *The New York Times*, September 7, 2017. Accessed at https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html?_r=0.

³ Op-Ed: *Raising Our Guard vs. Mega-Breaches*, Eric T. Scheniderman, Attorney General of New York State, *New York Daily News*, September 15, 2017. Accessed at <http://www.nydailynews.com/opinion/raising-guard-mega-breaches-article-1.3496434>.

⁴ *Equifax Stock Sales Are the Focus of U.S. Criminal Probe*, Tom Schoenberg, Anders Melin and Matt Robinson, *Bloomberg News*, September 18, 2017. Accessed at <https://www.bloomberg.com/news/articles/2017-09-18/equifax-stock-sales-said-to-be-focus-of-u-s-criminal-probe>.

⁵ *After the Equifax Breach, Consumers Were Advised to Freeze Their Credit, But Almost No One Did*, Lauren Lyons Cole, *Business Insider*, September 26, 2017. Accessed at www.businessinsider.com/equifax-credit-freeze-2017-9.

⁶ In recent years, American consumers have seen massive data breaches, including at national retailer Target, 1.5 billion Yahoo accounts compromised, and more than 22 million individuals' records held by the U.S. Office of Personnel Management.

the FTC received almost 400,000 identity theft complaints.⁷ The US Department of Justice reports that the actual number of Americans who are victims of at least one identity theft attempt or incident is significantly greater—an estimated 17.6 million in 2014—than logged with the FTC.⁸

While identity thieves run the gamut from family members and acquaintances taking personal information, to dumpster divers, to sophisticated computer hacks, this type of crime is enabled by the frequent, insecure availability and exchange of personally identifiable digital data and loose practices in opening credit. Indeed, an emerging trend flagged by the FTC in its 2017 recap of 2016 complaints was using consumer data to commit tax fraud—where a name and social security number are used to hijack an electronically filed tax return.⁹

In many cases, identity theft turns lives upside down, with 61% of victims reporting spending 40 or more hours to address (if not resolve) the resulting problems; some needing to turn to the government for assistance; missing work; loss of credit and other financial opportunities, including employment; significant stress and anxiety; impacts on family and other relationships; and out-of-pocket expenses.¹⁰ While many cases can resolve relatively quickly, others may drag on for years, with victims hounded by the fear borne of experience that another bill run up by a thief will suddenly appear.¹¹

It bears repeating that credit bureaus and other data companies have built their brand and their fortune on compiling and selling our personal information—usually without our permission. They profit by selling reports to creditors, employers, debt collectors and others. Consumers are indispensable to this business model, yet ironically unwitting bystanders in the relationship between data companies and their customers. Further irony is that this is all justified for the benefit of the consumer or to make the marketplace competitive.

Recommendations

NYPIRG starts from some fundamentals of consumer protection. First, it's our data and we should have control over it. Before our personally identifiable information is

⁷ *FTC Releases Annual Summary of Consumer Complaints*, March 3, 2017. Accessed at www.ftc.gov/news-events/press-releases/2017/03/ftc-releases-annual-summary-consumer-complaints.

⁸ *Why So Few Identity Theft Victims Turn to the Government for Help*, Andrea Peterson, *The Washington Post*, January 28, 2016.

⁹ The IRS reported that the incidence of tax return fraud in 2016 dropped by 46% to 376,000 cases. *IRS Identity Theft Plunges as Criminals Blocked from Stealing Refunds*, CBS News, March 9, 2017. Accessed at <https://www.cbsnews.com/news/identity-theft-taxpayer-refunds-drops-irs-security-push/>.

¹⁰ *Identity Theft: The Aftermath 2016*, Identity Theft Resource Center. (Survey of 300 identity theft victims from 40 states.) Accessed at http://www.idtheftcenter.org/images/page-docs/AftermathFinal_2016.pdf.

¹¹ *Id.*

taken and used, we should provide affirmative consent. Second, information taken for one purpose, like resolving a dispute, should not be used for another purpose, like issuing credit.

While credit monitoring and fraud alerts can be useful, the gold standard is to lock down your credit through a freeze. On a system-wide level, credit bureaus and others who routinely handle and use our sensitive personally identifiable information must be closely regulated and should be held accountable so that the corporate focus is shifted from near-term profit to longer range consumer protection. Since consumers are the injured parties, but don't directly buy the services of data companies, they cannot "vote with their feet" by choosing a competing product or service, as they might with another product or service that proved to be shoddy. In short, financial accountability through compensating victims and regulatory and/or civil fines must be greater than the cost savings from cutting corners on data security.

While we learn more about this latest data breach and consider policy options, NYPIRG recommends the Senate Consumer Protection Committee should advance the the following:

- Free, no restrictions freeze for all New Yorkers, without regard to whether they've been an identity theft victim.¹²
- Free, unlimited thaws, whether for particular credit issuers, for a specific time window or for all credit sources.
- Restore consumers' control over their financial information by establishing a "Default Credit Freeze," where consumers would have to affirmatively opt in to thaw/opt in affirmatively to approve release of their credit information.
- State promotion of the free freeze/lift/thaw through mailings and communications with public, e.g., tax refunds.
- Tighter corporate notice triggers to DFS and AG.
- Ban on upper management stock trades when they know or should know of breach.
- Furnish any additional powers to Department of Financial Services so they have all needed regulatory, investigatory and audit powers for consumer data companies.

We appreciate the opportunity to share our thoughts on this important area.

¹² NYPIRG supports Senator Elizabeth Warren's legislation (S.1816, introduced 9/14/17) to make credit freezes, temporary or full lifts/thaws free for all consumers. *See Elizabeth Warren's Equifax Bill Would Make Credit Freezes Free, CNN Money*, Robert Mclean, September 15, 2017. Accessed at <http://money.cnn.com/2017/09/15/pf/warren-schatz-equifax/index.html>.



AARP New York

**Testimony before the
Senate Committee on Consumer Protection:
Identity Theft**

**September 28, 2017
11:00 a.m.**

**Legislative Office Building
Hearing Room A
Albany, New York**

Introduction

Good morning Senator Carlucci and members of the committee. My name is Laura Ehrich and I am AARP's Associate State Director for Outreach and Engagement for New York State. I also serve as the state lead for fraud and scam education. AARP is a social mission organization with a membership of over 2.6 million members in New York State. Thank you for allowing me to testify on an issue that affects thousands of older New Yorkers and their families. I would like to submit the following testimony.

This hearing comes at a crucial time as news of the most recent data breach is foremost in people's minds. It's tragic that a person could work their whole life to build a nest egg for retirement and begin their next chapter, only to lose their hard-earned money to identity theft. The loss of money later in life is devastating because seniors simply lack the time to make up for the loss.

Background

Identity theft is a broad term for a variety of crimes that include the fraudulent acquisition and use of a person's private identifying information, like Social Security number, usually for financial gain. Access to personal identifying information may allow the imposter to obtain credit, open accounts, or make purchases in the victim's name.

People whose identities have been stolen can spend months or years and thousands of dollars cleaning up the damage that has been done to their good name and credit record. In the meantime, victims of identity theft may lose job opportunities, be refused loans for education, housing, or cars, and even get arrested for crimes they didn't commit.

To make matters worse, financial exploitation of older adults is the most common form of elder abuse and it is a growing problem in New York State and across the country.

AARP members are deeply concerned and believe that these disturbing trends need to be stopped. Statistics show how prevalent and devastating this issue is. For instance:

- The incidence of identity theft rose 16% between 2015 and 2016 alone, and cost consumers nationwide a total of \$16 billion in 2016.
- Seniors are frequently targeted by scammers. A report by the Federal Trade Commission (FTC) indicated that 36%, or more than one-third, of people aged 50 or older, have fallen prey to identity thieves.

According to the FTC for the year 2016, credit card fraud topped the list of ID theft complaints lodged by New Yorkers. The following table shows the various ID theft complaints by our fellow New Yorkers. A full table on other fraud complaints is attached along with an AARP infographic on Identity Fraud for your review.

Identity Theft Complaints Count from New York Victims = 20,205

Identity Theft Types Reported by New York Victims

Rank	Identity Theft Type	Complaints	Percentage¹
1	Credit Card Fraud	7,381	37%
2	Employment- or Tax-Related Fraud	5,516	27%
3	Phone or Utilities Fraud	2,870	14%
4	Bank Fraud	2,476	12%
5	Government Documents or Benefits Fraud	1,260	6%
6	Loan or Lease Fraud	1,172	6%
	Other	2,834	14%
	Attempted Identity Theft	55	<1%

¹Percentages are based on the 20,205 victims reporting from New York. Note that CSN identity theft complaints may be coded under multiple theft types.

AARP Fraud Watch Network and Outreach Campaign

Vigilance is one of the most powerful tools we have to stop frauds and scams. To that end, AARP created the Fraud Watch Network to empower people to identify and avoid scams. The

AARP Fraud Watch Network is a free resource to help you protect yourself and your family from identity theft and scams. Anyone of any age can access:

- The latest scam alerts, delivered right to your inbox;
- A scam tracking map featuring warnings from local law enforcement and first-hand accounts of breaking scams from people in your state;
- The Con Artist Playbook – interviews with con artists who reveal how they steal your hard-earned money; and
- A fraud hotline you can call to talk to a trained volunteer for advice if you are worried you or a loved one has been scammed or if you suspect a scam in your community. This volunteer-staffed hotline is a valuable tool providing a peer-to-peer experience. This is important because of the stigma attached to being the victim of a scam or fraud. Our volunteers can help callers determine next steps to mitigate the damage, and direct them to the appropriate agency to report the scam.
- In addition, we have a speakers' program with AARP volunteers and staff who can provide in-person presentations on identity theft, online and cyber security, investment scams, online dating scams, and more.

Conclusion

On behalf of AARP, I commend you for holding this important hearing to focus more attention on this critical problem of Identity Theft. AARP stands ready to work with you on educating New Yorkers on this problem and to find further solutions to help people combat this growing issue. I will be happy to answer any questions.



September 26, 2017

**Testimony of Leita King, MSW
Fraud, Scams, ID Theft Prevention Program Coordinator
Upstate Elder Abuse Center
Lifespan of Greater Rochester**

NYS Senate Special Standing Committee on Consumer Protection ID Theft

I would like to address my remarks to the following: Protection of older New Yorkers from scams, frauds and those who prey on them. Additionally, I would like to address the highly successful efforts Lifespan of Greater Rochester has been able to implement to prevent and intervene in these tragic situations.

Identity theft, along with fraud and scams, is prevalent in our service area of western NY. I am sure that the committee members are aware that older adults are by no means the only victims of fraud, scams and ID theft but they are often targeted by perpetrators. A federal report from the Bureau of Justice Statistics, *Victims of Identity Theft*, reported that the number of identity theft victims age 65 or older increased to 2.6 million nationally in 2014— up from 2.1 million in 2012.

Recent common scams in our region have been the grandparent scam, the contractor scam, the computer repair scam, Jamaican lottery and the IRS scam. Scams often involve the disclosure of financial and other personal information which leaves clients vulnerable to subsequent identity theft. In some cases, the purpose of the fraudulent encounter is to secure personal information for the purpose of opening fraudulent credit card accounts.

Lifespan is a not-for-profit social agency in Rochester that offers over 30 programs to help older adults take on the challenges and opportunities of longer life. It has been actively involved in helping older adults take on abuse, neglect and exploitation since 1986 when the Elder Abuse Prevention Program was formed. Since 2000 Lifespan has offered a Fraud and Scams Prevention Program which provides outreach and education to older adult groups and to professionals who work with them. The program also offers individual guidance and support for those who have fallen victim to fraud, scams and ID Theft. In 2011, Lifespan was awarded a grant from the Maryland Crime Victims Resource Center (MCVRC), acting as a grant manager for US DOJ Office for Victims of Crime, to launch an Identity Theft Coalition in eight Finger Lakes counties in New York State. Lifespan collaborated with adult protective services, aging service providers, law enforcement, district attorney offices, legal service providers, financial institutions, IRS and the NYS Attorney General's office to work together on prevention activities and to offer mitigation services to older victims of ID theft.

The grant also allowed Lifespan to develop a step-by-step Guide for Victims of ID Theft. It is available online and in print form and is used throughout New York State.

As the coordinator of Lifespan's Fraud, Scams and ID Theft Prevention Program which is housed in our Upstate Elder Abuse Center, I conduct group presentations to many groups of older adults and to professionals throughout our multi-county region. In 2016 this included over 1,900 older persons in seven Finger Lakes counties who attended presentations on avoiding victimization by fraud, scams and identity theft. I also worked on 102 cases of individual victims. A grant from the National Identity Theft Assistance Center has enabled us to expand our services to four more counties in western NY this year.

Fraud, scams and ID theft can leave older adult victims impoverished and confused. The impact is not limited to financial consequences. The actions needed to rectify this form of exploitation are often complicated and protracted. Victims often need much guidance and advocacy. I have frequently had to spend hours on the phone helping them call credit card companies, banks, and law enforcement and have accompanied older victims to court to seek justice for their losses. The loss of funds can mount to tens of thousands and even hundreds of thousands of dollars in some cases, leaving victims unable to pay for housing, taxes, and for

other essentials. Depression, anxiety and frustration are too often the unseen mental health consequences of the exploitation for older victims.

I'd like to provide a few examples of scam cases that have plagued older adults in Western NY. Unfortunately, the cases are not infrequent and often have devastating effects on the entire family system.

I worked with an 82-year-old man who believed he had won 2.5 million dollars and a Mercedes. He began corresponding by phone and mail with various scammers claiming to be with the lottery. This older adult began taking out cash withdrawals from the bank, wiring money through western union and using pre-paid debit cards to pay for alleged taxes and international fees. The scammer's sent my client a fake check for \$10,000 which he cashed and was then responsible for repaying. The scammer's called 10- 23 times daily, and it was later discovered they had reversed the charges. This older adult lost approximately \$79,000 and faced emotional and physical impacts due to the stress and devastation of the encounter. Lifespan provided guidance, support and assisted in contacting the necessary authorities to ensure this older adult was properly represented and protected.

I also worked with a 76-year-old woman who thought she had received a call from her grandson. The impersonator claimed he was in trouble and hurt due to a minor car crash in which the Police found pills in the car. This scammer begged her not to contact anyone, as he wanted to speak with his parents face to face. Another scammer came on the line claiming to be a Police officer and stated her grandson would spend the weekend in jail if his \$1,200 bail was not wired immediately. This older adult was deceived with fear and love for her grandson, being kept isolated with the request not to tell anyone and the immediacy of the request. Unfortunately, this older adult did wire the \$1,200 before speaking with her daughter. Lifespan was able to provide resources, guidance and support for the family.

Lifespan has also developed printed materials and magnets to alert the older adult population, their families and caregivers about the risks of victimization and to educate them about sources of assistance.

Lifespan is grateful for the funding it has received from NYS through the Office for the Aging and other government and non-governmental sources to do the important work of protecting older adults from all forms of exploitation. We also welcome the efforts of the Special Standing Committee to shine a spotlight on this issue. I would be happy to have more extensive discussions with members of the committee on the impact of ID theft on older adults and the role of state government in protecting older New Yorkers from the unlawful use of their personal information. Thank you for the opportunity to testify on this critical matter.

Leita King, MSW
Fraud, Scams & ID Theft Prevention Program Coordinator
Lifespan of Greater Rochester
1900 Clinton Ave. S.
Rochester, NY 14618
(585) 244-8400 x171
lking@lifespan-roch.org

A Summary of the Testimony of Maria Alvarez,
Executive Director, New York Statewide Senior Action Council

Maria Alvarez is Executive Director of Statewide Senior Action Council. Its board is consumer directed and consumer governed. This is a summary of her testimony.

Ms. Alvarez noted that in the internet age, consumers are faced with new and often frightening concerns. She noted that she has heard from many the fear they cannot trust anything anymore. Older New Yorkers are particularly effected. They are facing a world where more and more business is being conducted online.

Many seniors prefer to embrace new technology, but over half choose not to use the internet. Many who do use the internet want to use social media to connect with family or engage in online banking. This is set against the backdrop of many banks and many other businesses, encouraging people to do most of their businesses online.

Alvarez noted that it can be a challenge to ensure seniors that their personal information is secure online. It is even more difficult to assure seniors that their data is protected and it is now common to conduct business online when things like the Equifax breach happen. She has heard many questions coming from the community, particularly regarding the breach's effect on people's credit scores and about the risk of identity theft. She has seen sadness from many that this violation has happened.

Ms. Alvarez wants to see positive solutions. The challenge, in her view, is that though New York has online protections in place, the internet is global in scope. She believes we need to find a way in this climate to contain damages and to ensure that there are reparations for New Yorkers, including older New Yorkers, who have been aggrieved.

Ms. Alvarez stated government must seek interdisciplinary, intergovernmental solutions. Outreach and education must be a component of any actions taken. In her view, government is not presently doing this, due to the fear of cost inefficiency and an aversion to spending on social causes.

In her view, any outreach must include print media since not everything is easily accessible via the internet for many people. Face-to-face meetings with people in the community are also effective. It goes a long way toward ensuring that people are not so scared

Ms. Alvarez also pointed out that anyone – not just seniors – can be scammed online, no matter how tech savvy they may be. To make matters worse, scammers are often a few steps ahead.

Finally, Ms. Alvarez noted that elder abuse and financial exploitation costs seniors \$3 billion in New York alone. She states that even this is a very conservative amount because many do not report when they are scammed and abused.

She concluded that there is a need for more community programs focused on education and outreach. On policy side, government must work at all levels to insure that there is accountability

and verification of who persons online are claiming to be. Government must work to effect more interdisciplinary investigations and solutions.



CDIA

CONSUMER DATA INDUSTRY ASSOCIATION
Empowering Economic Opportunity

Writer's Direct Dial: 202.408.7407

Writer's email: cellman@cdiaonline.org

September 26, 2017

The Honorable David Carlucci
Chair, Senate Committee on Consumer Protection
Albany, NY 12247

Re: Hearing on Identity Theft

Dear Chairman Carlucci:

On behalf of the Consumer Data Industry Association ("CDIA"), please accept this written testimony for your committee's upcoming hearing to investigate how best to protect consumers, such as seniors and internet users, from the theft of their personal information.

CDIA is an international trade association, founded in 1906, of more than 130 corporate members. Its mission is to enable consumers, media, legislators and regulators to understand the benefits of the responsible use of consumer data which creates opportunities for consumers and the economy. CDIA members provide businesses with the data and analytical tools necessary to manage risk. They help ensure fair and safe transactions for consumers, facilitate competition and expand consumers' access to a market which is innovative and focused on their needs. CDIA member products are used in more than nine billion transactions each year.

We realize that the hearing falls on the heels of an announcement by Equifax that, during a criminal hack, data on approximately 143 million consumers had been compromised. CDIA cannot address the specifics of this attack, of course, but we can address the federal and state obligations that regulate our members, and we can address the importance of CDIA member data for social good.

We want to make your committee aware of several points. First, there are many substantial laws that regulate CDIA members. Second, the data that CDIA members compile and use are often done to promote social good. Third, there many substantial laws to prevent and remediate identity theft.

1. Federal and state law regulating data

A. *The Fair Credit Reporting Act*

First and foremost, CDIA members are consumer reporting agencies and are heavily regulated by both the Federal Fair Credit Reporting Act (“FCRA”) and the New York Fair Credit Reporting Act (“New York FCRA”).¹ The FCRA governs consumer reports, regulates consumer reporting agencies, and protects consumers. The law requires consumer reporting agencies to maintain reasonable procedures to assure maximum possible accuracy.² The law also provides many other consumer protections as well. For example:

- Those that furnish data to consumer reporting agencies cannot furnish data that they know or have reasonable cause to believe is inaccurate, and they have a duty to correct and update information.³
- Consumers have a right to dispute information on their consumer reports with consumer reporting agencies and the law requires dispute resolution within 30 days (45 days in certain circumstances). If a dispute cannot be verified, the information subject to the dispute must be removed.⁴
- A consumer reporting agency that violates federal law is subject to private lawsuits and enforcement by the Federal Trade Commission (“FTC”), Consumer Financial Protection Bureau (“CFPB”), and state attorneys general.⁵

Then-FTC chairman, Tim Muris, said “[t]he FCRA is an intricate statute that strikes a fine-tuned balance between privacy and the use of consumer information. At its core, it ensures the integrity and accuracy of consumer records and limits the disclosure of such information to entities that have ‘permissible purposes’ to use the information.”⁶

¹ 15 U.S.C. § 1681 et seq.; N.Y. Gen. Bus. L. § 380 et seq.

² *Id.*, § 1681e(b).

³ *Id.*, § 1681s-2(a)(1) - (2).

⁴ *Id.*, § 1681i(a)(1), (5).

⁵ *Id.*, § 1681n, 1681o, 1681s.

⁶ FTC Chairman Tim Muris, Oct. 4, 2001 before the Privacy 2001 conference in Cleveland (“Muris statement”).

B. *The Gramm-Leach-Bliley Act (“GLBA”)*

Many CDIA members are “financial institutions” under federal law and because of this designation, they are regulated by Title V of the Gramm-Leach-Bliley Act (“GLBA”).⁷ Title V established privacy and data security duties for financial institutions. The Federal Trade Commission (“FTC”) is the enforcement agency with the power to investigate companies for compliance under GLBA. As the FTC noted

Many companies collect personal information from their customers, including names, addresses, and phone numbers; bank and credit card account numbers; income and credit histories; and Social Security numbers. The Gramm-Leach-Bliley...Act requires companies defined under the law as ‘financial institutions’ to ensure the security and confidentiality of this type of information. As part of its implementation of [GLBA], the [FTC] issued the Safeguards Rule, which requires financial institutions under FTC jurisdiction to have measures in place to keep customer information secure.⁸

Among other things, regulated entities must develop a written information security program appropriate to its size and the complexity, the nature and scope of its activities, and the sensitivity of the customer information at issue; and they must adopt written policies and procedures addressing administrative, technical, and physical safeguards for the protection of customer records and information.

Violations of the GLBA Safeguards Rule are enforced by the FTC and the FTC has brought more than a dozen actions against institutions under its jurisdiction for violation of the Safeguards Rule. The privacy and data security duties under the GLBA contribute to reducing risks for consumers.

C. *CFPB Supervision*

As part of the Dodd-Frank Act⁹, the CFPB supervises the nationwide credit bureaus. The CFPB regularly issues reports about its supervision of credit bureaus and other participants in the credit reporting system. The CFPB has noted that its

work is producing an entirely different approach to ensuring compliance at the major consumer reporting companies: one of proactive attention to compliance, as opposed to a defensive, reactive approach in response to consumer disputes and

⁷ 15 U.S. Code §§ 6801 – 6809.

⁸ *Financial Institutions and Customer Information: Complying with the Safeguards Rule*, FTC, <https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-compliance>.

⁹ Also known as the Wall Street Reform and Consumer Protection Act (Pub.L. 111–203).

lawsuits. This proactive approach to compliance management will reap benefits for consumers – and the lenders that use consumer reports – for many years to come.¹⁰

The power to supervise comes with the power to enforce. As the CFPB has noted,

[w]hen Supervision examinations determine that a supervised entity has violated a statute or regulation, Supervision directs the entity to implement appropriate corrective measures, such as implementing new policies, changing written communications, improving training or monitoring, or otherwise changing conduct to ensure the illegal practices cease. Supervision also directs the entity to send consumers refunds, pay restitution, credit borrower accounts, or take other remedial actions.¹¹

As but one example of corrective action in the credit reporting ecosystem, the CFPB noted in 2017 that it

directed both bank and nonbank furnishers to develop reasonable written policies and procedures regarding accuracy of the information they furnish and to take corrective action when they furnished inaccurate information. In addition, we took significant steps to ensure furnishers' dispute handling processes comply with the law in response to failures either to conduct investigations or to send results of dispute investigations to consumers.¹²

D. Unfair or deceptive trade practices

Under both federal and state law, all CDIA members are prohibited from engaging in unfair or deceptive trade practices.¹³ By 2016, the FTC has brought more than 60 data security cases and in so doing, it has built a strong body of common law through settlements with affected companies. Relying on its authority from 15 U.S.C. § 45(a), which prohibits "unfair ... practices in or affecting commerce," these settlements identified problematic practices and provided guidance to other companies on how the FTC viewed the concept of "reasonable and appropriate" data security.

¹⁰ *Supervisory Highlights Consumer Reporting, Special Edition, Issue 14, Winter 2017, 2*, http://files.consumerfinance.gov/f/documents/201703_cfpb_Supervisory-Highlights-Consumer-Reporting-Special-Edition.pdf ("CFPB Winter 2017 Highlights").

¹¹ *Supervisory Highlights, Issue 15, Spring 2017, 1*, http://files.consumerfinance.gov/f/documents/201704_cfpb_Supervisory-Highlights_Issue-15.pdf.

¹² CFPB Winter 2017 Highlights, 3.

¹³ 15 U.S.C §§ 41-58.

E. Breach notification laws

Federal breach notification standards are included in the Interagency Guidance for banks and credit unions.¹⁴ State law governs how breach notifications occur for businesses, including consumer reporting agencies.

F. Death Master File

The National Technical Information Service (“NTIS”), under the U.S. Department of Commerce, makes the Death Master File (“DMF”) available to those who qualify. Under 2013 changes to federal law, there are new restrictions on access to the DMF.¹⁵ Under these new restrictions there must be a certification that a receiving entity (1) has systems, facilities and procedures in place to safeguard DMF data; and (2) has experience in maintaining the confidentiality, security and appropriate use of such data, under requirements similar to those under existing law.¹⁶ Subscribers are also subjected to periodic audits.

G. Drivers Privacy Protection Act

Some CDIA members are also covered entities under the Drivers Privacy Protection Act¹⁷ (“DPPA”)¹⁸. This statute prohibits the release and use of certain personal information from state motor vehicle records.

H. Financial services providers

Many CDIA members are service providers as defined by the Dodd Frank Act.¹⁹ The CFPB has issued a bulletin describing their extensive expectations for banks and financial institutions to oversee these providers. CDIA members are subject to extensive oversight by their customers of their ability to comply with federal consumer financial laws, including data security practices under GLBA, Title V.

¹⁴ *Interagency Guidelines Establishing Information Security Standards*, Federal Reserve Board of Governors, <https://www.federalreserve.gov/bankinfo/reg/interagencyguidelines.html>.

¹⁵ Bipartisan Budget Act of 2013, Pub. L. 113-67, § 203.

¹⁶ 26 U.S. Code § 6103 (confidentiality and disclosure of tax returns and tax return information).

¹⁷ 18 U.S.C. § 2721

¹⁸ 18 U.S.C. 2721.

¹⁹ 26 U.S.C. § 2002(26).

I. *Other relevant laws and standards*

There are other relevant laws and standards that regulate and guide our industry. These laws and standards include:

- CDIA members that are publicly traded on U.S. exchanges are subject to Sarbanes-Oxley data security requirement which is part of the audit of a company's controls.²⁰
- Through contractual requirements and voluntarily standards, many CDIA members are compliant with the Payment Card Industry Data Security Standard (PCI DSS).
- Through contractual requirements and voluntarily standards, many of our members are compliant with the ISO/IEC 27001 standard. "The ISO/IEC 27001 is the best-known standard in the family providing requirements for an information security management system (ISMS). An ISMS is a systematic approach to managing sensitive company information so that it remains secure. It includes people, processes and IT systems by applying a risk management process."

2. **Data for good**

We urge that your committee take a thoughtful and cautious approach before considering limits on the access to data since limits on data access could increase fraud and slow down consumer transactions. CDIA members use information every day for the public good. Our members use information by government to prevent tax and public assistance fraud; to help banks and retailers prevent identity theft; to assist child support enforcement agencies in locating deadbeat dads; and to help law enforcement locate victims, witnesses, and fugitives.

CDIA member data are used to empower economic opportunity by allowing consumers to obtain mortgages, car loans, and student loans at any hour of the day from their living rooms. CDIA member data are used by consumers to open in-store, instant credit to obtain discounts on clothes, electronics, appliances, or other consumer goods.

The chairman of the FTC was right when he referred to the "miracle of instant credit" whereby a consumer can walk in to an auto dealer and "can borrow \$10,000 or more from a complete stranger, and actually drive away in a new car in an hour or less." Chairman Muris also noted that this

²⁰ 15 USC § 7262 (also known as Sec. 404 of the Sarbanes-Oxley Act, Pub. L. 107-204).

'miracle' is only possible because of our credit reporting system. The system works because, without anybody's consent, very sensitive information about a person's credit history is given to the credit reporting agencies. If consent were required, and consumers could decide - on a creditor-by-creditor basis - whether they wanted their information reported, the system would collapse.²¹

Public records maintained by CDIA members are often used by law enforcement and state and local government agencies. The cost increases for public records imposed on our members would increase for all those using public records databases, like law enforcement, state agencies fighting fraud, and even lawyers and courts doing research and investigations. Examples of the public good for CDIA member data include the following:

- FBI Director Louis Freeh testified before Congress in 1999 and noted that in 1998, his agency made more than 53,000 inquiries to commercial on-line databases "to obtain public source information regarding individuals, businesses, and organizations that are subjects of investigations." This information, according to Director Freeh, "assisted in the arrests of 393 fugitives, the identification of more than \$37 million in seizable assets, the locating of 1,966 individuals wanted by law enforcement, and the locating of 3,209 witnesses wanted for questioning."²²
- The Association for Children for Enforcement of Support reports that public record information provided through commercial vendors helped locate over 75 percent of the "deadbeat parents" they sought.²³
- "We [the Texas Attorney General's Office] need the private sector [which also includes public record information] to help protect consumers and help combat identity fraud. Moreover, we also need the private sector to assist law enforcement."²⁴

3. Laws to prevent and remediate identity theft

There are many laws to prevent and remediate identity theft and a list of many of these laws and regulations are attached. A few are highlighted in this comment. Under

²¹ Muris statement.

²² *Hearing before the Senate Comm. on Appropriations Subcomm. for the Departments of Commerce, Justice, and State, and the Judiciary and Related Agencies, March 24, 1999* (Statement of Louis J. Freeh, Director of the Federal Bureau of Investigation).

²³ *Information Privacy Act, Hearings before the Comm. on Banking and Financial Services, House of Representatives, 105th Cong., 2nd Sess.* (July, 28, 1998) (statement of Robert Glass).

²⁴ *Amicus Argument of James Ho for State of Texas, Taylor v. Acxiom Corp.*, U.S. Court of Appeals (5th Cir.) Case Nos. 08-41083, 41180, 41232, (Nov. 4, 2009).

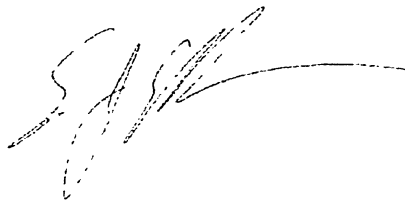
state law, any consumer has a right to place a credit freeze on their credit report.²⁵ This credit freeze should prevent the opening of new credit in the consumer's name. Under federal law, consumers can also block from appearing on a credit report, any item that was compromised by fraud that appears on the identity theft report.²⁶ Consumers who believe they are identity fraud victims can request that a fraud alert be placed on their credit reports to signal to prospective users of that report that the consumer may be a fraud victim.²⁷ There are also obligations on lenders and creditors. For example, federal banking agencies and users of consumer reports (i.e. lenders) must establish red flag guidelines to better identify fraud patterns.²⁸

Summary

CDIA is deeply troubled that one of our members was the subject of a criminal intrusion that resulted in compromise of data on approximately 143 million consumers. We hope that your committee can take a step back and look at the larger picture. This attack should not taint an entire industry. We request that your committee keep three points in mind. First, there are many substantial laws that regulate CDIA members. Second, the data that CDIA members compile and use are often done to promote social good. Third, there many substantial laws to prevent and remediate identity theft.

I would be happy to meet with you and other committee members to discuss CDIA's position in greater detail.

Sincerely,

A handwritten signature in black ink, appearing to read 'Eric J. Ellman', with a long horizontal flourish extending to the right.

Eric J. Ellman
Senior Vice President, Public Policy & Legal Affairs

Enclosure

²⁵ N.Y. Gen. Bus. L. § 380-t.

²⁶ 15 U.S.C. § 1681c-2.

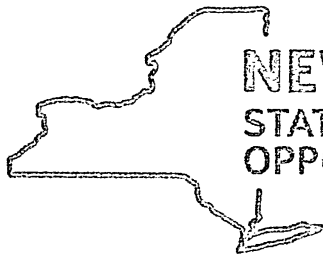
²⁷ *Id.*, § 1681c-1.

²⁸ *Id.*, § 1681m(e).

Summary of ID Theft Solutions
in the
Federal Fair Credit Reporting Act (FCRA)
15 U.S.C. Sec. 1681 et seq.

- *Free Credit Reports.* Consumers are entitled to one free credit report per year under the following circumstances:
 - When an active duty member of the military places an active duty alert on his credit report. 15 U.S. Code § 1681c-1(c).
 - One free per year, per national credit bureau. 15 U.S. Code § 1681j(a).
 - Any time a consumer receives an adverse action notice. 15 U.S. Code § 1681j(b).
 - One free per year if the consumer is unemployed and seeking employment. 15 U.S. Code § 1681j(c)(1).
 - One free per year if the consumer is on public assistance. 15 U.S. Code § 1681j(c)(2).
 - One per year if the consumer has reason to believe that the file on the consumer at the agency contains inaccurate information due to fraud. 15 U.S. Code § 1681j(c)(3).
 - When a consumer places an initial fraud alert on her credit report, which a consumer can do every 90 days. 15 U.S. Code § 1681j(d).
 - When a consumer places an extended fraud alert on her credit report, which lasts for seven years. 15 U.S. Code § 1681j(d).
- *Tradeline Blocking.* Consumers with an identity theft report, as that term is defined by law, can block from appearing on a credit report, any item that was compromised by fraud that appears on the identity theft report. 15 U.S.C. § 1681c-2.
- *Fraud Alerts and Active Duty Alerts.*
 - Consumers who believe they are identity fraud victims can request that a fraud alert be placed on their credit reports to signal to prospective users of that report that the consumer may be a fraud victim. 15 U.S.C. § 1681c-1.
 - Consumers who are on active military duty away from their duty station may request that an active military duty alert be placed on their credit reports to signal to prospective users of that report that the consumer may be not be the actual applicant for credit. 15 U.S. Code § 1681c-1(c).
- *Social Security Number Truncation.* Consumers may request that consumer reporting agencies truncate their SSNs on credit reports. 15 U.S. Code § 1681g(a)(1)(A).
- *Credit and Debit Card Number Truncation.* Merchants must truncate debit and credit card account numbers on receipts. 15 U.S.C. § 1681c(g).
- *Establishment of Red Flag Guidelines.* Federal banking agencies and users of consumer reports (i.e. lenders) must establish red flag guidelines to better identify fraud patterns. 15 U.S.C. § 1681m(e).
- *Summary of Rights.* Consumer reporting agencies must provide to consumers a summary of their rights if they become identity fraud victims. 15 U.S.C. § 1681g(d).
- *Complaint Coordination.* The FTC and national consumer reporting agencies must develop a system to coordinate consumer complaints. 15 U.S.C. § 1681s(f).

- *Prevention of Reappearance of Fraudulent Information.* Companies that furnish data to consumer reporting agencies must develop procedures to prevent the reappearance of data that was subject to fraud. 15 U.S.C. § 1681s-2(a)(6).
- *Debt Collection.* Debt collectors collecting for a third party must, when notified by a consumer that the collection item is the subject of fraud, inform the company for whom the collector is collecting of the alleged fraud. In addition and upon request, the collector must share with the consumer information relative to the debt. 15 U.S.C. § 1681m(g).
- *Statute of Limitations Extension.* The statute of limitations against consumer reporting agencies, and users of information from and furnishers of information to consumer reporting agencies is extended to two years from the date of the discovery of the violation or five years from the date the cause of action arises. 15 U.S.C. § 1681p.
- *Studies on Identity Fraud.* The Treasury Department is required to conduct an identity fraud study. Pub. L. 108-159, Sec. 157.
- *Enhanced Opt-Out from Pre-approved Credit or Insurance Offers.* New easier and simplified method lenders use to inform consumers of their right to remove their names from pre-approved credit or insurance offer lists. In addition, the timeframe for opt-out is extended from two to five years. 15 U.S.C. § 1681m(d).
- *Disposal of Records.* FTC and federal banking agencies to develop rules concerning the disposal of credit records. 15 U.S.C. § 1681w, 16 CFR 682.3.
- *Reporting of Negative Information to Consumer Reporting Agency.* Lenders must inform consumers that negative information may be reported to consumer reporting agencies 15 U.S.C. § 1681w.
- *Enhanced Obligations on Furnishers to Report Accurate Information.* 15 U.S.C. § 1681i(a)(5)(A).
- *Address Reconciliation.* Consumer reporting agencies must notify users of consumer reports about a substantially different address between an address on an application and an address on the credit report. Users must have policies to handle this situation under regulations from federal banking agencies. 15 U.S.C. § 1681c(h).



**NEW YORK
STATE OF
OPPORTUNITY.**

**Department
of State**

New York State Senate Hearing:

**“Examine Identity and Personal Information Theft
Scams Over the Internet and Discuss Best Practices to
Protect Consumers from These Threats”**

Testimony for Submission to:

The Senate Committee on Consumer Protection

September 28, 2017

Albany, New York

Andrew M. Cuomo
Governor

Rossana Rosado
Secretary of State

INTRODUCTION

Thank you for the opportunity to provide testimony to the Senate Standing Committee on Consumer Protection concerning identity and personal information theft scams over the Internet and best practices to protect consumers from these threats.

The Department of State is deeply concerned by reports surrounding the Equifax breach, and committed to doing everything possible to ensure that consumers across the State of New York are protected. At the direction of Governor Cuomo, New York State took swift action in response to the breach by issuing emergency regulations that would require credit reporting agencies to register with New York for the first time and comply with this state's first-in-the-nation cybersecurity standard. The Administration will continue to act to ensure that New Yorkers have the resources they need to make informed and responsible decisions around their personal information. We appreciate the Legislature's commitment to addressing this issue and would welcome the opportunity to discuss legislative options that would further safeguard the rights of New Yorkers.

THE THREAT OF IDENTITY THEFT

Identity theft is a serious threat in today's digitized economy – impacting millions of people every year. The Bureau of Justice Statistics reports that 17.6 million Americans were victims of identity theft in 2014 alone. While identity theft crimes vary, from taking control of existing accounts to opening new accounts, the vast majority of identity theft victims experience the misuse of an existing credit card or bank account.¹

¹ https://www.bjs.gov/content/pub/pdf/vit14_sum.pdf

While anyone is vulnerable to identity theft, the Department’s Division of Consumer Protection (the “Division”) is acutely concerned about the State’s vulnerable children and elderly populations. Children are estimated to be 35 times more likely to be victimized than adults.² The theft of a child's identity may go unnoticed for years; most child victims only become aware of their stolen identities when they decide to open a bank account, apply for a job, seek credit, rent an apartment, or apply for a student or car loan. Likewise, financial elder abuse yields staggering economic consequences; estimates range from almost \$3 billion to more than \$30 billion annually depending whether unreported crimes are considered.³ Quantifying the exact nature of the frauds targeting the elderly is difficult because the crimes often go unreported. In fact, a 2011 study conducted in New York State found that in one year only 1 in 44 cases was reported.⁴ A more recent 2016 New York State study examined 479 verified cases of fraud reported from October 1, 2012 to September 30, 2013 and estimated both reported and unreported claims to be a staggering \$109 million.⁵

THE DEPARTMENT’S ROLE IN PROTECTING CONSUMERS

The Department of State plays an important role in safeguarding consumer rights, and is working to bring to bear the full resources and authorities of the agency to do so. The Division is charged with the interrelated duties of educating the State’s consumers about, and protecting them from, scams and fraud in today’s robust marketplace. This includes: (1) providing direct assistance and mediation to resolve marketplace complaints; (2) providing mitigation assistance

² *Child Identity Theft Report 2012: What to Know*, All Clear ID, (May 1, 2012).

³ National Council on Aging, “Top 10 Scams Targeting Seniors”, available at <https://www.ncoa.org/economic-security/money-management/scams-security/top-10-scams-targeting-seniors/>

⁴ *Under the Radar: New York State Elder Abuse Prevalence Study*, (May 2011).

⁵ *The New York State Cost of Financial Exploitation Study*, Office of Children and Family Services (June 15, 2016).

to victims of identity theft; (3) conducting educational campaigns related to scam prevention, identity theft prevention, financial literacy, and product safety; (4) advancing cost effective and quality electric, gas, telephone, and cable service by representing consumers at utility rate and policy proceedings before New York State and Federal regulators; and (5) enforcing New York State's Do Not Call Law (the "DNC Law").

The Division has prioritized educational programming to best equip New Yorkers with the knowledge and skills necessary to recognize and thwart fraud and scams before they occur. In 2016, the Division delivered 132 presentations to community groups, organizations, and educational institutions across the State. The Division's Outreach and Education Unit is currently presenting the *S.A.F.E. Senior Anti-Fraud Education, Identity Theft and Scam Prevention*, and *Safeguarding Your Child's Identity* programs at a variety of venues. The *S.A.F.E.* program describes the top eight common scams directed at seniors, provides scam prevention tips, and steps to take if someone is victimized by a scam. The *Identity Theft and Scam Prevention* program provides consumers with important prevention tools to safeguard one's identity and tips for spotting a scam before becoming a victim. Likewise, the *Safeguarding Your Child's Identity* program provides parents and caregivers with critical security freeze information to secure your child's financial record.

The Division's website has a myriad of tools and information to aid consumers. We frequently update the webpage dedicated to scam alerts and trends, which currently features information about more than 20 known scams. The Division posts the information and sends alerts via social media to warn consumers whenever new scams are uncovered.

In addition, the Division's Consumer Assistance Hotline is available to New York's consumers Monday through Friday from 8:30 a.m. to 4:30 p.m. to answer consumers' questions, mediate and resolve complaints and assist in identity theft mitigation. Consumers also have the option of filing a consumer complaint electronically 24 hours per day, seven days per week, via the Department's website.

RESPONSE TO THE EQUIFAX DATA BREACH

In response to the Equifax data breach, Governor Cuomo directed the promulgation of emergency regulations to require credit reporting agencies to register with the State of New York and comply with this state's first-in-the-nation cybersecurity standard.

The Department of State is committed to playing its part in ensuring that all New Yorkers who may have been impacted by the Equifax breach have access to the resources they need to make informed, responsible decisions about their personal information. On September 7, 2017, the Division received notice from Equifax that it suffered a data security breach on July 29, 2017 affecting over 8.3 million New Yorkers. The information accessed by the hackers included consumers' names, birthdates, Social Security numbers, driver's license numbers, credit card numbers, and "dispute documents" containing personal information. In response, the Department took several important steps and has worked to deploy the full range of resources at its disposal. First, the Division made available the Consumer Assistance Hotline to field calls and educate concerned New Yorkers seeking assistance in responding to the breach—nearly 650 consumer inquiries have come in through the month of September. Second, in coordination with the Department of Financial Services, the Department has worked to develop consumer outreach

materials, which we plan to deploy widely. Lastly, the Division remains in contact with Equifax to elicit necessary information to best inform and protect New York consumers affected by the Equifax breach.

We appreciate the legislature's commitment to addressing this critical topic, and we look forward to future discussions with the Senate on how best we can work together to safeguard the rights of New Yorkers. As Governor Cuomo has said, we cannot "sit idly by while New Yorkers remain unprotected."



Consumers Union Demands Equifax Make Affected Customers Whole

The policy and mobilization arm of Consumer Reports is deeply concerned and outlines fixes the company must make

By Octavio Blanco
September 14, 2017

Consumers Union, the policy and mobilization arm of Consumer Reports, sent a letter to Equifax CEO Richard Smith on Thursday, expressing deep concern over the immediate and lasting effects for the 143 million consumers potentially compromised by the data breach the company announced last week.

In the letter, the consumer advocacy organization called Equifax's response "wholly inadequate" and outlined seven steps it believes Equifax must take to remediate the situation, including paying for credit freezes, processing disputes promptly, and setting aside funds to compensate consumers.

"Given the extraordinary nature of this breach and the threat posed to nearly half of all Americans, Equifax has a responsibility to offer consumers the best resources and tools to help them protect themselves," said Jessica Rich, vice president of Policy and Mobilization at Consumers Union.

Consumer Reports reached out to Equifax late afternoon for reaction to the demands and will update the story with any comments.

The credit bureau today did provide some more details about the breach, saying on its website, "We know that criminals exploited a U.S. website application vulnerability," adding that it was working with law enforcement.

Equifax also said that customers affected by the breach who have signed up for free credit monitoring will not be subjected to a binding arbitration clause.

On Sept. 7, Equifax, one of the big three credit monitoring bureaus, announced that it had been aware—since July—that it was the victim of a massive hack affecting more than 100 million accounts.

According to Equifax, the information exposed included Social Security numbers, birth dates, addresses, and in some instances, driver's license numbers. In addition, Equifax said the credit card numbers of approximately 209,000 consumers and certain dispute documents, which included personal identifying information, for approximately 182,000 consumers, were accessed.

MORE ON THE EQUIFAX DATA BREACH

[Security Freeze vs. Fraud Alert: Deciding the Best Option Could Changing Your Social Security Number Protect You From Equifax-Related Fraud?](#)

[How to Lock Down Your Money After the Equifax Breach](#)

Equifax says it moved quickly to help people potentially impacted by the breach. The credit bureau says it took steps to stop the intrusion, engaging an independent cybersecurity firm to forensically investigate the breach. The cybersecurity firm Equifax hired will also determine the scope of the hack and provide recommendations to help prevent a similar incident in the future.

Equifax also established a dedicated website, www.equifaxsecurity2017.com, where it provides a tool for users to determine if their information may have been stolen. The company is also offering U.S. consumers an identity theft protection and credit file monitoring product called TrustedID Premier, free for one year. It includes credit monitoring of Equifax, Experian, and TransUnion credit reports; copies of a user's Equifax credit report; the ability to lock and unlock an Equifax credit report; and identity theft insurance. The company will also scan the internet for Social Security numbers. Users must enroll by November 21, 2017.

Consumers Union says these steps don't go far enough. ([Read the full text of the letter.](#))

CU: What Equifax Should Do

1. Pay for credit freezes. “Consumers who wish to freeze their credit in response to Equifax’s announced breach still must pay to freeze their records with other major credit bureaus in order to make the freeze effective. We urge Equifax to pay any fees associated with credit freezes at other credit bureaus so that consumers can prevent their data from being improperly used in connection with other credit bureau records,” Consumers Union said.

2. Extend credit monitoring for affected consumers. Consumers Union points out that Equifax has offered affected consumers “only one year of credit monitoring and, following public outcry, a limited and narrow opportunity to obtain a free credit freeze.” Because risks to consumers due to this breach are not limited to one year,

Consumers Union demands that "Equifax should extend credit monitoring indefinitely for all consumers potentially affected by the breach."

3. Provide more detailed information about the security incident. Consumers Union says the company provided "inadequate and unreliable information" about which consumers were victimized and what data was compromised, limiting consumers' ability to take steps to protect themselves. "To prevent further harm to consumers seeking to protect themselves, Equifax must upgrade its tool to provide more detailed information about precisely what types of data were breached for each affected consumer," Consumers Union said.

4. Remove all mandatory arbitration clauses. Equifax has been criticized for forcing victims visiting its site to waive their right to sue the company. Equifax says that it has corrected this issue, but Consumers Union says the remedy is confusing and insufficient. "Equifax has repeatedly changed its story about whether and how the mandatory arbitration clause impacts consumers," the letter said.

For example, after Equifax said its arbitration clause was moot, Consumers Union notes that another—broader—arbitration clause remained in effect. According to Consumers Union, Equifax is now saying that none of these clauses will apply to consumers harmed by the data breach or who sign up for credit monitoring services. However, the clauses remain in print and, Consumers Union says, "it's unclear whether or how they could still be used to prevent consumers from having their day in court."

5. Commit to hiring and training sufficient staff to review and process disputes promptly. “Given the enormity of the exposure, Equifax needs to be prepared for a deluge of problems and must have sufficient resources on hand to resolve these problems quickly and effectively,” Consumers Union said. “The company should not wait for these problems to pile up and then address a mounting backlog.”

6. Set aside a fund to compensate consumers whose data has been exposed. “Equifax has an obligation to American consumers to compensate them for the injury they may incur for years to come. Accordingly, Equifax should create a substantial and dedicated reserve account to compensate consumers affected by this breach,” Consumers Union wrote.

7. Investigate allegations of insider trading and hold wrongdoers accountable. “The company does not appear to have fully investigated—and certainly has not explained to the public—the sales of stock by three executives just prior to public announcement of the breach,” Consumers Union said. “The timing of these sales—a handful of days after the initial uncovering of a massive security incident—raises major red flags. However, Equifax’s initial reaction was disappointing and troubling: first, its press statement sought to minimize the scope of \$2 million in sales as ‘small.’ Second, rather than stating an intention to investigate the issue, Equifax casually and summarily dismissed the allegation of trading on nonpublic information with no apparent inquiry at all—much less a rigorous one.”

Consumers Union says that Equifax should immediately act to preserve all documents and communications of the

executives in question, and commit to an independent investigation of the possibility of insider trading.

What's Next

The letter concludes with an acknowledgment of the magnitude of the fast-moving situation, but stresses that “the consumers injured by this breach should be the company’s first and foremost priority, and Equifax should commit to their protection and to making them whole.”

The Equifax CEO is scheduled to testify before the House Energy and Commerce committee on October 3. That committee has jurisdiction over the Federal Trade Commission and Consumer Financial Protection Bureau, the agencies responsible for regulating data security.

On Thursday the FTC announced that it had launched an investigation into the Equifax breach.

"The FTC typically does not comment on ongoing investigations. However, in light of the intense public interest and the potential impact of this matter, I can confirm that FTC staff is investigating the Equifax data breach," Peter Kaplan, the FTC's Acting Director of Public Affairs, told Consumer Reports in an email.

Also, Connecticut Attorney General George Jepsen has announced that his office has initiated a formal multi-state investigation into the breach.

Buy right every time

Subscribe for unlimited access to ratings and reviews

Subscribe

© 2006 - 2016 Consumer Reports

A Credit Freeze Won't Help With All Equifax Breach Threats

There are other dangers you should know about. Here's how to protect yourself.

By Jeff Blyskal
September 19, 2017

If you've placed a security freeze on your credit reports at Equifax, Experian, TransUnion, and Innovis, that will help prevent fraudsters from opening new credit accounts in your name.

Freezing your credit report specifically at Equifax will also prevent crooks from registering as you at the government website, my Social Security, and block them from attempting to steal your Social Security benefits.

But taking these steps won't protect you against *every* identity fraud threat arising from the Equifax data breach.

With the information that hackers got, including access to Social Security numbers, birth dates, and an unspecified number of driver's license numbers, you need to take other steps to help lock down your finances.

Here are three important ways you can protect yourself.

Buy right every time

Subscribe for unlimited access to ratings and reviews

Subscribe

Tax Refunds

With your Social Security number, crooks can file false income tax returns in your name, take bogus deductions, and steal the resulting refund. More than 14,000 fraudulent 2016 tax returns, with \$92 million in unwarranted refunds, were detected and stopped by the Internal Revenue Service as of last March.

MORE ON EQUIFAX DATA BREACH

[How to Lock Down Your Money After the Equifax Breach](#)
[Consumers Union Demands Equifax Make Affected Customers Whole](#)

[Security Freeze vs. Fraud Alert: Deciding the Best Option](#)
[How to Freeze Your Credit While Applying for a Loan](#)

Though you are generally not liable for such fraud, if a criminal manages to change your tax records and receive your refund, it can take months to straighten out the mess.

How to protect yourself. The best defense is to obtain an Identity Protection PIN from the IRS, which is a code that must be filed with your legitimate return for it to be accepted. An identity thief can't file his fraudulent return without your PIN.

But you can get a PIN only if a fraudulent return has previously been filed in your name, if the IRS determines that

you're an ID-fraud victim, or if you live in a high tax-related identity theft locale such as Washington, D.C.; Florida; or Georgia.

The IRS would not say whether those affected by the Equifax breach would qualify for a PIN.

Andrew Mattson, a tax partner at the Moss Adams tax firm in Silicon Valley, recommends that taxpayers who don't officially qualify for a PIN request one anyway, by filing a Form 14039, Identity Theft Affidavit (PDF). "Even if the IRS says no, your account will generally be flagged for additional monitoring for suspicious activity," he says.

Mattson also recommends that you periodically view your IRS account information, which shows when returns were filed and which refund payments were made. Activity there—if it's not yours—can be a sign of fraud. The balance updates every 24 hours, usually overnight, but there is a one- to three-week lag in the time it takes for refund payments to show up.

If you suspect fraud, contact your local IRS office using the Taxpayer Assistance Center Office Locator.

Health Insurance

Data from the Equifax breach can be used to steal your benefits from private health insurance, Medicare, or Medicaid when the identity thief uses your coverage to pay for his own medical treatment and prescriptions.

Many health insurers have internal special investigation units and anti-fraud personnel to root out medical identity fraud,

and if suspicious activity is detected, they'll send email alerts to the policyholder, says Cathryn Donaldson, a spokeswoman for America's Health Insurance Plans, the trade association of health insurers.

How to protect yourself. Get copies of your medical records from providers to establish the baseline of your health before your records are compromised.

Increasingly, online patient portals make this easy to do. Check back regularly to see whether providers you didn't use are listed and whether you've been charged for treatments you never received.

In addition, review your free annual MIB Consumer File, which contains medical and personal information about you reported by health, life, disability, and other member insurers. Do the same for your Milliman Intelliscript report, which tracks your history of prescription drug purchases.

The Federal Trade Commission also says consumers should ask each of their health plans and medical providers for the "accounting of disclosures" related to their medical records. That tells who got copies of your records from the provider. The law allows you to order one free copy from each medical provider every year.

If available, sign up for your insurer's secure online portal, and regularly review the explanation of benefits, which shows which treatments you received when and from which providers. While there, sign up for fraud alerts via email or text message, which will keep you apprised of benefit payments.

Regularly review your credit report for medical collection accounts that don't belong to you.

Your Driver's License

Using your driver's license number, identity thieves can create bogus driver's licenses and hang their moving violations on you. With more work and information from phishing or further hacking, identity thieves can create bogus checks to pay a cashier, who "verifies" the shopper's identity by writing your license number on the bad check.

If this happens to you, you may not discover how your license has been used until a police officer tells you, or perhaps, until a bank closes your account because of too many bounced checks.

How to protect yourself. Ask the motor vehicles department to give you a copy of your driving record; most states charge for this, usually about \$10. To find out whether any bad checks are attributed to your driver's license, request your free annual consumer report from each of the big three check verification companies, ChexSystems, Certegy, and TeleCheck.

If you find that your driver's license is being used fraudulently, you can file a police report at your local police department and ask the motor vehicles department to flag your license number, which will alert law enforcement officers to be extra careful in identifying people they pull over with your license number. You should also request a new driver's license number.

If you're arrested or find criminal charges on your record, go to the Identity Theft Resource Center for advice on clearing criminal identity theft; if you find fraudulent checks on your record, follow the ITRC for advice on resolving checking account fraud. You can also call the center at 888-400-5530 for free assistance.

Correction: A previous version of this article said people should register at the government website my Social Security to protect their Social Security benefits. In fact, setting up a credit freeze with Equifax will stop identity thieves from setting up a my Social Security account in your name.

© 2006 - 2016 Consumer Reports

ConsumersUnion*

POLICY & ACTION FROM CONSUMER REPORTS

September 14, 2017

Richard F. Smith
Chairman and Chief Executive Officer
Equifax, Inc.
1550 Peachtree Street, NE
Atlanta, GA 30309

Dear Mr. Smith:

Consumers Union, the policy and mobilization division of Consumer Reports,¹ is an expert, independent, nonprofit organization whose mission is to work for a fair, just, and safe marketplace for all consumers and to empower consumers to protect themselves. We write to express our deep concern about both the immediate and lasting effects of the devastating breach that was announced by Equifax on September 7, 2017.

Your company has estimated that the breach compromised the highly sensitive information—including social security numbers, driver's license numbers, and birthdates—of potentially 143 million consumers, nearly half of the U.S. population. The compromise of this information, apparently by malicious hackers determined to misuse it, leaves all affected consumers vulnerable to identity theft and other fraudulent uses of their information for years to come.

We recognize that Equifax, and likely many law enforcement agencies, are still investigating the facts surrounding the breach, as well as the question of whether Equifax had reasonable policies and protocols in place to protect the highly sensitive consumer data it collects, stores, and sells. However, it is clear that Equifax's response to date has been wholly inadequate. Your company has offered affected customers only one year of credit monitoring and, following public outcry, a limited and narrow opportunity to obtain a free credit freeze. The company provided inadequate and unreliable information about which consumers were victimized and what information was compromised, limiting consumers' ability to take steps to protect themselves. Equifax also originally forced victims visiting its site to waive their rights to

¹ Consumer Reports is the world's largest independent product-testing organization. It conducts its policy and mobilization work in the areas of telecommunications reform, as well as financial services reform, food and product safety, health care reform, and other areas. Using its more than 50 labs, auto test center, and survey research center, the nonprofit organization rates thousands of products and services annually. Founded in 1936, Consumer Reports has over 7 million subscribers to its magazine, website, and other publications.

sue the company for the harms caused and, following public outcry, has not fully corrected this problem. Further, the company does not appear to have fully investigated—and certainly has not explained to the public—the sales of stock by three top executives just prior to public announcement of the breach.²

Given the extraordinary nature of this breach and the threat posed to nearly half of all Americans, Equifax has a responsibility to offer consumers the best resources and tools to help them protect themselves. We call on Equifax to take the following additional steps to help remediate the serious harm and ongoing risks to consumers:

1. Pay for credit freezes.

Security experts agree that the most effective remedy in the event of the exposure of sensitive data such as social security numbers is a credit freeze. By prohibiting others from accessing their credit records without permission, consumers can take control over their identity in the wake of a breach.

When it announced the breach, Equifax did not initially offer free credit freezes to affected consumers. Then, fully five days later, and only in response to massive public outcry, Equifax announced on September 12 that it was waiving Equifax credit freeze fees for the next 30 days. However, that window of time is still far too short, as consumers still have very little information about the extent of the breach. We urge Equifax to extend this waiver indefinitely and to clarify that (1) consumers who were previously charged will be automatically refunded and (2) Equifax will not charge consumers for subsequent actions to unfreeze and refreeze their records.

Moreover, consumers who wish to freeze their credit in response to Equifax's announced breach still must pay to freeze their records with other major credit bureaus in order to make the freeze effective. Many creditors, for example, consult only one credit bureau for a loan applicant. The sensitive personal information compromised in the breach can thus be used to fraudulently obtain credit and cause other harm without Equifax being contacted. We urge Equifax to pay any fees associated with credit freezes at other credit bureaus so that consumers can prevent their data from being improperly used in connection with other credit bureau records.

2. Extend credit monitoring for affected consumers.

² Other missteps that should and could have been avoided include: 1) the PIN generated for an Equifax credit freeze should not have been a timestamp of when the consumer requested it 2) consumers should not have been asked for credit card information in order to sign up for free credit monitoring, and 3) Equifax hosted information about the breach on www.equifaxsecurity2017.com, an irregular and easily spoofed domain.

To date, Equifax has offered one year of free credit monitoring to consumers possibly affected by the breach. Credit monitoring provides less protection than a credit freeze, but does provide useful and immediate information that could be used to limit the consequences of identity theft after the fact. However, the risks to consumers due to this breach are not limited to one year—data exposed to hackers could be used to open fraudulent accounts several years in the future. For this reason, Equifax should extend credit monitoring indefinitely for all consumers potentially affected by the breach. If Equifax subsequently determines that there is a reasonable likelihood that sensitive data such as a social security number has been breached for certain consumers, Equifax should extend its credit monitoring for those consumers for life.

3. Provide more detailed information about the security incident.

While Equifax has been aware of the security incident since July, it has to date provided only very vague information about the breach and about what consumer data was compromised. The initial Equifax statement confusingly stated that while the breach “potentially impact[s] 143 million consumers,” the company’s core consumer and commercial credit databases were unaffected. Providing more information about *which* databases were compromised could help consumers and regulators determine how best to respond.

Moreover, while consumers have been told that the compromised databases *include* information such as social security numbers, email addresses, financial account information, and birth dates, there is no way for consumers to determine what particular data elements were exposed about each of them individually. Equifax has provided a tool for consumers to see if they were compromised, but that tool only indicates “we believe that your personal information may have been impacted by the incident,” with no indication of what information was or was likely exposed. Further, consumers have reported inconsistencies in the tool, such as providing different responses for the same personal information submitted through different devices, or indicating likelihood of compromise for invented and implausible names.

To prevent further harm to consumers seeking to protect themselves, Equifax must upgrade its tool to provide more detailed information about precisely what types of data were breached for each affected consumer. Knowing what data was exposed can guide consumers in choosing which steps, in addition to security freezes and credit monitoring, they must take to avert additional forms of identity theft, such as medical or tax fraud. If this tool cannot be fixed or replaced, it should be taken offline immediately, so that consumers do not rely on inaccurate information to their detriment.

Finally, while we understand that the causes of the breach are still under investigation, we call on Equifax to commit to a full public explanation and accounting of the compromise, and what security measures and procedures were in place to protect consumer data. Given the

sensitivity of the data that Equifax holds, the importance of this data in granting or denying important consumer benefits, and the fact that consumers have little or no control over either, Equifax has a heightened responsibility to be fully transparent about what has happened, in order to minimize the damage and forestall similar episodes going forward.

4. Remove all mandatory arbitration clauses.

When Equifax announced the breach, its terms of use for the credit monitoring tool stated in fine print that consumers were waiving their rights to sue and instead would submit to mandatory arbitration. Imposing this condition on victims of the breach was met with strong public criticism, and for good reason—forced arbitration deprives consumers of access to public courts of law, undercutting fundamental legal protections.

Equifax has repeatedly changed its story about whether and how the mandatory arbitration clause impacts consumers. Following public outcry when consumers and the media noticed the clause, Equifax announced that it would apply only to the special new credit monitoring service, and not to the breach itself. Even then, another arbitration clause remained in effect for other consumers who signed up for its existing credit monitoring service. Further, all consumers who interact in any way with the site remained subject to yet *another*—and far broader—binding arbitration provision purporting to cover “any claim, dispute, or controversy between You and Us relating in any way to Your relationship with Equifax.” Equifax is now saying that none of these clauses will apply to consumers harmed by the data breach *or* who sign up for credit monitoring services. However, the clauses have not been removed and could be changed at any time, so it is still unclear whether or how they could still be used to prevent consumers from having their day in court.

Equifax does a huge disservice to consumers by including mandatory arbitration clauses in boilerplate legal terms forced on consumers. While the information that Equifax collects, stores, and sells play a vital role in the U.S. economy, consumers do not generally make a choice about providing it, and have little opportunity to hold Equifax and the other credit bureaus accountable. Equifax should not try to insulate itself from accountability even further by forcing consumers into private, company-selected panels that operate in secret and are not bound by law or legal precedent.

5. Commit to hiring and training sufficient staff to review and process disputes promptly.

Given the enormity of the exposure, Equifax needs to be prepared for a deluge of problems, and must have sufficient resources on hand to resolve these problems quickly and

effectively. The company should not wait for these problems to pile up and then address a mounting backlog. In addition to hiring more call support staff to address consumer inquiries, Equifax should act now to hire and train the staff needed to keep any backlog from occurring. Equifax should also commit to resolve disputes promptly, consistent with the requirements under federal law.³

6. Set aside a fund to compensate consumers whose data has been exposed.

As Equifax investigates the full extent of this breach, it will gain a better sense of the potential long-term risks to consumers for identity, tax, and medical fraud. Equifax has an obligation to American consumers to compensate them for the injury they may incur for years to come. Accordingly, Equifax should create a substantial and dedicated reserve account to compensate consumers affected by this breach.

7. Investigate allegations of insider trading and hold wrongdoers accountable.

Finally, we have followed news reports that three senior Equifax executives sold a significant amount of Equifax stock after the internal discovery of the data breach on July 29, but before it became known to the public or to regulators. The timing of these sales—a handful of days after the initial uncovering of a massive security incident—raises major red flags. However, Equifax’s initial reaction was disappointing and troubling: first, its press statement sought to minimize the scope of \$2 million in sales as “small.” Second, rather than stating an intention to investigate the issue, Equifax casually and summarily dismissed the allegation of trading on nonpublic information with no apparent inquiry at all—much less a rigorous one. It seems surprising that the Chief Financial Officer of the company would not have been notified in advance of the massive liability exposure the breach posed for the company. Equifax should immediately act to preserve all documents and communications of the executives in question, and commit to an independent investigation of the possibility of insider trading.

³ The Fair Credit Reporting Act generally requires that disputes be resolved within 30 days. 15 U.S.C. § 1681i(a)(1)(A).

Conclusion

Although we understand that Equifax is adapting in real time to a fast-moving situation, the consumers injured by this breach should be the company's first and foremost priority, and Equifax should commit to their protection and to making them whole. There is much more that could and should be done in light of the significant risks to consumers caused by this enormous breach. We urge Equifax to address the many concerns discussed above, and to continue to look for new ways to protect consumers from the potentially catastrophic harm this breach could cause.

Sincerely,

Jessica Rich
Vice President, Policy and Mobilization

Justin Brookman, Director, Consumer
Privacy and Technology Policy

Consumers Union
1101 17th Street, NW
Suite 500
Washington, DC 20036

How to Lock Down Your Money After the Equifax Breach

Don't panic. Follow these 4 steps to protect your assets and credit.

By Jeff Blyskal

Last updated: September 12, 2017

If you haven't already, the first, best, and fastest way to protect yourself from the Equifax data breach is to place a security freeze on your credit files at the big three credit reporting bureaus.

"A security freeze is the nuclear option of credit protection. It gives maximum protection," says Matt Schulz, a senior security analyst at CreditCards.com.

Consumers should apply the freeze to Equifax, and also to Experian, and TransUnion. For extra security, you can apply a freeze to a fourth, lesser-known consumer reporting agency, Innovis.

You can do this by contacting each bureau either through their website or through the customer service number. Depending on where you live, there may be a fee for placing the freeze.

The company, however, said this week it would not charge for credit freezes for those affected by the breach.

The massive data breach, announced Thursday by Equifax, involves the potential compromise of the personal data of 143 million consumers, including names, addresses, Social Security numbers, and birth dates.

Anxious consumers have since flooded Equifax's website and customer service lines, and many had trouble determining from the site if their information was among the data that had been stolen.

Equifax faced additional scrutiny from the New York State Attorney General's office on Friday. The AG was concerned about language in the terms of use for a credit monitoring service Equifax is offering free to consumers concerned about the breach. The terms of use suggested that signing up for the credit monitoring service would subject consumers to binding arbitration, which could prevent them from joining a class-action suit against Equifax.

Late Friday, Equifax said in a news release that it was fixing its website so customers could more easily determine if their information had been compromised. The release also specified that the binding arbitration clause and class-action waiver were only applicable to the credit monitoring services, and did not apply to the data breach.

Equifax later dropped the restrictions for the free credit-monitoring service as well, claiming that customers who sign up because of the data breach are not subjected to the clause and would not be prevented from joining class action suits.

Many details about the data breach are still unclear, but the potential consequences for consumers are severe.

"In total, the data elements breached provide a toolkit for financial fraud," says Beth Givens, executive director of the Privacy Rights Clearing House, which has tracked data breaches since 2005.

Identity thieves can link this information to "over a billion passwords stolen elsewhere to piece together a more complete profile of you" to commit financial crimes, says Avivah Litan, a security analyst at Gartner, a technology research firm.

In addition to the credit freeze, there are four more steps to put an iron wall around your money.

Activate Two-Factor Authentication

In today's world of digital crime and internet fraud, two-factor authentication is an important extra layer of safety. It requires not just a password but a second element, such as a code texted to your smart phone, which *you* have but a crook can't easily get. Set up and activate two-factor authentication on all of your existing mobile banking, savings, credit card, home equity line of credit, and other financial accounts that offer it.

Most banks that offer mobile banking also authenticate the device you use to access your account, says Doug Johnson, senior vice president of payments and cybersecurity at the American Bankers Association.

Banks with the most cutting-edge security, such as USAA, use yet another factor, biometric authentication, which verifies your identity by using your fingerprint or voice print, or through facial recognition-which criminals can't easily fake.

Maximize Your Mutual Fund Security

Although the Securities and Exchange Commission requires mutual funds companies to identify, detect, and respond to red flags of identity theft, unlike FDIC-insured banks, these investment firms aren't required to restore assets stolen by hackers.

You should call your 401(k) plan provider and other investment managers to learn their fraud protection policies, as they can vary from company to company. If your investment company doesn't explicitly reimburse stolen funds, consider moving your money elsewhere.

The two biggest investment companies, Fidelity and Vanguard, have voluntary online fraud policies that promise to reimburse assets stolen in unauthorized online transactions.

To get protection, Vanguard requires (and Fidelity requests) that you follow certain safeguards, which you should be doing anyway, including regularly reviewing your account statements and promptly reporting any errors or suspected fraud; keeping up-to-date security on any computer or other device you use to access your account (firewall, antispyware, and antivirus software); not responding to, clicking a link in, or opening an attachment in an e-mail that you suspect might be fraudulent and that requests personal financial information; and using two-factor authentication.

Place a Fraud Alert on Credit Reports

A fraud alert is different from a credit freeze. The fraud alert is a notice on your credit report that warns both current and prospective lenders that they must take reasonable steps to verify your identity before granting credit, such as a new credit card or loan, or extending credit on an existing account.

You need to request a fraud alert at one of the big three credit bureaus, which will then pass it on to the other two, and separately place another alert with Innovis. An alert lasts 90 days. If you're an ID-theft victim, you can get a fraud alert that stays in place for seven years. But you may be better off with the 90-day alert, because that allows you to get a free credit report from each of the four credit bureaus each time you renew the alert, which means you can get up to 16 free reports per year.

Secure Your Smartphone + Email

How you manage your smartphone and email accounts can be critical to your online security. Your phone is where all your second-factor text message codes are sent and where your mobile banking and other money apps live. Email is where your financial institutions send alerts and password reset links.

Hackers can hijack your phone and access important information, but "it's difficult, and if you take only one extra step, a hacker will pass you up and try elsewhere," says Roger

Entner, founder of Recon Analytics, a telecom research firm. Here's how you can make your phone and email harder targets:

- Activate two-factor authentication on your email account. When you log into your email on an unfamiliar computer or phone, you'll get a text with the necessary code to complete login. A hacker would need that code, too, but can't get it without your phone. Better yet, download an authenticator app such as Google Authenticator or Microsoft Authenticator, which generates these codes without the need for texts, which can be intercepted.
- Use a password management app such as LastPass on your computer's browser and on your phone, advises Russell Vines, Consumer Reports' director of information security. LastPass creates and plugs different passwords into each of your accounts when you log in, so you don't have to invent and keep track of dozens of passwords. This eliminates the temptation of using the same password for multiple accounts, which can provide a master key for hackers.
- Never click unsolicited, unexpected, or suspicious-looking links sent to you by email or text. They could download malware capable of spying on your phone or personal computer activity.
- Follow other security tips for your phone's specific operating system using the FCC Smartphone Security Checker, a customizable interactive tool.

Buy right every time

Subscribe for unlimited access to ratings and reviews

Subscribe

© 2006 - 2016 Consumer Reports

Security Freeze vs. Fraud Alert: Deciding the Best Option

The Equifax breach puts a new focus on both tools, but one is more effective

By Jeff Blyskal
September 13, 2017

The recent security breach at Equifax has left some 143 million consumers scrambling to understand the difference between fraud alerts and security freezes, and which works best in protecting their personal information.

The tools work in similar ways to prevent fraudulent use of your credit data, so it's easy to mix them up.

Equifax added to the general confusion by marketing its credit monitoring service to those seeking information about the breach. The terms of use appeared to subject consumers to binding arbitration, which would have prevented them from joining class-action lawsuits. Under pressure from regulators, the company removed the arbitration requirement.

If you're a victim of the Equifax breach, don't hesitate to use these tools to safeguard your information. You can opt for one or both, depending on what's right for your situation. Here's how to choose between a freeze and a fraud alert, and the best way to protect your credit.

Buy right every time

Subscribe for unlimited access to ratings and reviews

Subscribe

Security Freeze

A security freeze placed on your credit file will block most lenders from seeing your credit history. That makes a freeze the single most effective way to protect against fraud.

If a prospective lender can't pull your credit report, he won't issue a new loan. That usually stops identity thieves from setting up fraudulent accounts in your name.

There's a drawback, though. The freeze also shuts out most companies you may *want* to do business with, including lenders, telecom companies, and insurers.

To give them access when you want to apply for a loan or open a cellular service account, you have to temporarily lift the freeze and set a date for it to be reinstated automatically.

Not everyone is blocked from getting your credit report. Banks and credit unions where you already have accounts can still check your credit report, as well as collection agencies and certain government agencies.

A freeze might be free, depending on your state and circumstances—for example, if you're an identity-theft victim and have filed a police report about the incident. Otherwise,

expect to pay \$2 to \$12 to initiate or temporarily lift a freeze at each credit bureau: Equifax, Experian, TransUnion, and Innovis. Review your state's law for specific details.

Fraud Alert

A less restrictive option is a fraud alert, which is a notice placed on your credit report warning prospective lenders that you are a victim of identity theft. That means they should take reasonable extra steps to verify your identity before granting credit to the person claiming to be you.

To request a fraud alert, you have to contact only one of the big three credit bureaus— Equifax, Experian, or TransUnion. The bureau you contact will pass it on to the other two. (You must place a separate alert with Innovis, a smaller credit bureau.)

An initial fraud alert lasts 90 days. If you're an ID-theft victim, you can get a extended fraud alert that stays in place for seven years. But you may be better off with the 90-day alert because that allows you to get a free credit report from each of the four credit bureaus each time you renew the alert.

With these renewals, you can get 16 free reports per year in addition to the free annual credit report you're already entitled to from each of the bureaus. Getting 20 free credit reports a year allows you to keep a reasonably close eye on your file year-round and eliminates the need for costly credit monitoring.

Double Protection

For anyone who is in the middle of buying a home, or some other financial transaction, you may not want to block prospective lenders from seeing your credit file. If that's the case, opting for a fraud alert may offer reasonable protection, because lenders will be warned and you'll receive a free credit report from each bureau.

Still, a credit freeze is the stronger option. So if you can't lock down your credit now, plan on doing so as soon as you can.

And for maximum protection, we recommend using both freezes and fraud alerts. As the Equifax breach showed, you can't be too careful.



Could Changing Your Social Security Number Protect You From Equifax-Related Fraud?

Perhaps, but it's not a simple process, and you have to meet certain requirements

By Consumer Reports
September 13, 2017

Thieves got a goldmine of data when they stole 143 million Social Security numbers—along with names, addresses, and birth dates—belonging to Equifax customers. With it, they can steal property, money, get access to medical records, file fake tax returns, and wreak other havoc.

You might think an obvious way to protect yourself would be to change your Social Security number. But while you can easily change passwords, freeze accounts, and take other steps to keep your personal data secure, changing your Social Security number is complicated and not something anyone can do.

To make a change, you need a valid reason. Being a victim of identify fraud is an acceptable one, but you will have to submit proof that your current number is being misused and that the problem is an ongoing hardship.

Buy right every time

Subscribe for unlimited access to ratings and reviews

Subscribe

If you think you qualify for a new number, you'll need to keep records of anything that seems to indicate trouble, such as an IRS letter questioning you about income not reported, records of your frustrating battle to correct credit reports, or a letter denying you a mortgage because of erroneous information. If an identity thief filed a false tax return to steal your refund, that will certainly help your case.

If you have that information, you can get started by applying in person at a Social Security office. You'll need to complete the free application for an original Social Security card (Form SS-5). Here, you'll have to document the reason you need a new number, explaining how the old one has been compromised and how you have suffered.

You'll also need to prove your citizenship and identity with a valid drivers license or a U.S. passport, birth certificate, or other acceptable document.

MORE ON THE EQUIFAX DATA BREACH

[Equifax Data Breach: What Consumers Need to Know](#)

[How to Lock Down Your Money After the Equifax Breach](#)

[Equifax Sued Over Massive Breach; Company Criticized for Response to Theft](#)

The SSA will review your application but may also look to see whether you've taken other steps first to resolve your problem, such as placing a security freeze on your account, which can help shut the door on a crook trying to access your credit report.

Once the application has been received, the agency will decide whether to approve your request for a new number. If it does, you should get it within 10 to 14 business days, according to Nicole Tiggemann, a spokeswoman for the agency.

But keep in mind that even if you are given a new number, your old Social Security number won't go away. Instead, it will remain assigned to you and be linked to the new one.

The SSA will then send information about your new number to the IRS, your employer, and other federal agencies. But you may have to take on the task of updating others.

To make that process smoother, the Identity Theft Resource Center, a nonprofit organization established to support victims of identity theft, recommends that you get a letter from the SSA detailing the change and stating that you will no longer be using the old number.

Be aware that because your credit history is tied to your Social Security number, getting a new number could indicate to some companies that you don't have a credit history. That could happen, for example, if you apply for a mortgage or a credit card using your new number. In that case, you may have to explain that your Social Security number is linked to the older number that is connected to your credit-history data.

**Testimony of the Domestic Violence and Consumer Law Working Group
at Fordham Law School Feerick Center for Social Justice**

**NEW YORK STATE SENATE COMMITTEE ON CONSUMER PROTECTION
2017 NYS SENATE HEARING ON IDENTITY THEFT**

September 26, 2017

Prepared by: Divya Subrahmanyam, Esq.
Working Group Co-Chair
CAMBA Legal Services
Brooklyn, NY

Diane Johnston, Esq.
Working Group Co-Chair
The Legal Aid Society
Jamaica, NY

We are honored to submit this testimony for the New York State Senate Committee on Consumer Protections Hearing on Identity Theft. We are members of the Domestic Violence and Consumer Law Working Group—established and supported by Fordham Law School’s Feerick Center for Social Justice. The Working Group is made up of legal services attorneys specializing in consumer law and/or domestic violence and domestic violence service providers from organizations throughout New York City. In this testimony, we detail the specific needs and vulnerabilities of domestic violence survivors in the context of identity theft, the barriers to relief they face, and potential policy solutions for the Committee to consider.

Prevalence of Intimate Partner Identity Theft

Domestic violence is a leading cause of homelessness among women and women-headed households. It is also strongly associated with poverty. As the literature shows and practitioners know, creditworthiness is essential for domestic violence survivors to establish and maintain stable lives, free from abuse. The main reason cited by domestic violence survivors who are forced to return to their batterers is a lack of financial stability, often including lack of housing or the inability to obtain employment.

An estimated 98 percent of domestic violence survivors have experienced financial abuse,¹ which can take many forms, including preventing the victim from working or sabotaging work opportunities; controlling how money is spent or access to money; withholding money for necessities like food and shelter; creating debt burdens in the name of the victim; or refusing without grounds to pay bills in the victim’s name.

Intimate partner identity theft is one of the most common forms of financial abuse. It provides a way for abusers to derive financial benefit and maintain their control over their victims.² Current and former spouses and intimate partners often have open access to their partner’s personal identification information, including all of the information required to open a new line of credit or obtain other services: prior addresses, dates of birth, social security numbers, driver’s license numbers, passport numbers, checks, bank account numbers, and knowledge of the answers to security questions. Identity theft frequently includes making unauthorized charges on an existing account or using a victim’s personal information to open new accounts without their knowledge or permission. Abusers may also open a business in the victim’s name and amass debts related to the business, file false employment documents to increase business tax deductions, file other types of fraudulent tax documents, or use their children’s personal information to open accounts.

Severe Consequences for Domestic Violence Survivors

Unfortunately, many survivors do not discover identity theft until long after the relationship has ended. Frequently, they only find out about the crime at critical moments when they are denied vital necessities due to the identity theft; for example, when false wage information makes the victim appear ineligible for desperately needed public benefits, when

¹ NATIONAL NETWORK TO END DOMESTIC VIOLENCE, *About Financial Abuse*, <http://nnedv.org/resources/ejresources/about-financial-abuse.html>.

² PAULA PIERCE, OFFICE FOR VICTIMS OF CRIME TRAINING AND TECHNICAL ASSISTANCES CTR., IDENTITY THEFT RESOURCE PAPER 4 (2012), *available at* http://www.ncdsv.org/images/OVCTTAC_IdentityTheftResourcePaper_2012.pdf.

federal tax debts result in a denial for subsidized housing, or when the client's wages are garnished at a new job.

The impact of identity theft on a survivor's credit report can be even more devastating than for other consumers. When survivors have ruined credit or a low credit score, they are often unable to access housing, utilities, insurance, or obtain credit cards. New York state employers outside of New York City are permitted to check credit reports and scores when hiring, and they often do. With a ruined credit history, a survivor may not be able to find adequate housing or employment, or even be able to have a phone turned on. In the long term, a survivor with a poor work history will have a lower salary, less security, and fewer retirement funds. As a result, the survivor may find it difficult to exit shelter into stable housing, and may even contemplate returning to the abuser despite the dangers. In this way, economic abuse will be felt for years, if not decades.

Asserting identity theft and repairing its harm can take months and sometimes years. Victims of existing account fraud spend an average of 58 hours to repair the damage, and victims of new account fraud spend an average of 165 hours to redress the situation.³ Victims report emotional suffering as a result of this victimization, including feelings of embarrassment, anger and hopelessness, which is only heightened when the perpetrator is a friend or family member. For domestic violence survivors who are already dealing with the aftermath of trauma, the emotional distress created by identity theft is likely to be even more severe. They are forced to mentally revisit their abuse, to think about their abuser, and to recount their abuse over and over again, to creditors, credit reporting agencies, the police, and more. Survivors often worry about whether the abuser will discover that they are disputing the account, become angry, and try to locate them.

There are also serious safety concerns for survivors of domestic violence who are victims of identity theft. Financially savvy abusers can pull the credit report using personal identifying information known to them and see the new address listed by the domestic violence survivor. Advocates have described cases where abusers have pulled credit reports to track credit inquiries by prospective employers. Interference with employment is a common tactic used by abusers and can raise significant safety concerns.

Barriers to Relief

Access to Credit Reports

After learning of identity theft, the first step in pursuing relief is usually for a consumer to review his or her credit report for fraudulent activity. Unfortunately, accessing a credit report can be extremely difficult, and sometimes dangerous, for survivors of domestic violence.

Credit reporting agencies ("CRAs") commonly verify the identity of the person accessing the report by confirming the mailing address on file and by posing security questions derived from the information contained in the file of the very accounts that have been fraudulently

³ PIERCE, *supra* note 2, at 6. In a 2004 study, 39 percent of identity theft victims reported still dealing with the identity theft two years after discovered, while some victims reported dealing with the identity theft for more than ten years. *Identity Theft and Domestic Abuse*, ELEC. PRIVACY INFOR. CTR., https://www.epic.org/privacy/dv/identity_theft.html.

opened. While identity verification is essential to protecting consumers from fraud, these particular procedures make it especially difficult for victims of identity theft, including domestic violence survivors, to obtain their reports. They rarely know what accounts have been fraudulently opened in their names until they review their credit reports, which means that they cannot answer the security questions posed to access the reports online. Inaccurate address information then compounds the problem by impeding the process of ordering these reports by mail. We routinely see these difficulties prevent identity theft victims from obtaining their reports even when they provide accurate address information, photo identification and proof of social security number. In particular, even when survivors residing in shelter send a letter of residency from the shelter with their request, the credit reporting agencies reject this as inadequate proof of address. In our experience, domestic violence survivors are rarely able to access all three major credit reports as a result of this and other issues specific to survivors.

Because survivors of domestic violence are often unable to obtain a credit report after learning of potential intimate partner identity theft, they are excluded from pursuing any relief when CRAs, law enforcement, creditors and other entities erroneously require a copy of a credit report or a credit report number.

Access to Documentation

Once survivors are able to discover what accounts the identity thief has opened or used, they may theoretically turn to remedies provided by New York law and the federal Fair Credit Reporting Act, which can eliminate liability on an account or block accounts from a credit report.⁴

Most of these forms of relief, however, require a victim to obtain a law enforcement report. The law provides only a very broad definition of a law enforcement report broad, and the Federal Trade Commission (“FTC”) has created an Identity Theft Affidavit and Report, a sworn statement by the victim that is submitted to the FTC. However, in practice, creditors, credit reporting agencies, and New York courts often demand a police report, and will not grant relief without one. Obtaining a police report is difficult for survivors, and the requirement poses added barriers for survivors seeking to resolve the consequences of identity theft. In New York City, victims meet resistance when they attempt to report identity theft to the police. Police officers frequently refuse to take identity theft complaints, misunderstand what constitutes an identity theft crime, and make unreasonable demands on the types of documents a victim must provide in order to make a complaint.

Domestic violence survivors face even more challenges in obtaining reports or initiating investigations. Law enforcement often view reports of spousal identity theft as a domestic dispute, rather than the legitimate identity theft it is. They are especially reluctant to make such reports when the identity theft occurred prior to legal separation or divorce. Without a police report, victims face an uphill battle in repairing the damage caused by identity theft. They may be unable to block the information from appearing on the credit report, and may be held responsible for debts that are not theirs, or even sued on the debts and eventually forced to make payments.

⁴ N.Y. Gen. Bus. Law §§ 604-a, 339-e, 380-t and 15 U.S.C. § 1681, et seq., respectively.

The lack of a police report may also inhibit a survivor's ability to obtain a credit freeze. Ordinarily, it costs five dollars to lift or reinstate the freeze. Under New York law, these fees are waived for victims of domestic violence and victims of identity theft – with appropriate documentation, such as a law enforcement report or an order of protection.⁵ For survivors who are unable to get a police report, the fees for temporarily lifting and later reinstating the freeze while applying for housing can quickly add up. And because they frequently have fled the abuser with no access to funds, without fee waivers, the survivor's housing search and shelter stay is likely to be extended. In all these ways, survivors are often forced to choose between exposing themselves to increased danger or protecting themselves from identity theft.

Our Clients

Many survivors are unable to address the identity theft until after they have safely fled the abusive relationship; this is sometimes long after the fraud was committed, which makes obtaining relief even more challenging. Here, we provide the accounts of two of our clients who continue suffering the consequences of identity theft, even after finding an advocate.

Ms. I., a domestic violence survivor, first learned that she was a victim of identity theft in early 2014 when she began receiving letters from collections agencies for several credit cards and cell phones that her abusive ex-husband had opened in her name, both during their marriage and after they had separated. Ms. I. immediately sought assistance, but soon found she would need a police report to deal with the alleged debts completely. Throughout 2015, Ms. I. made a total of eight attempts to file a report with various law enforcement offices in New York City, but was denied each time. She was told multiple times, incorrectly, that because they had been married and lived together, her ex-husband had a right to use her personal information. After over a year of persistent efforts, Ms. I. decided to proceed with requesting a block using what little documentation she had. Her first attempts at obtaining the block were rejected by the original creditor and by the credit reporting agencies. Eventually, after her attorney helped her file a complaint with the Consumer Financial Protection Bureau, one CRA placed a block on the disputed information. The accounts continue to be reported by the other two.

Ms. L. sought out financial advocacy because she had begun to receive letters from credit card companies with whom she had no accounts. As she only speaks Mandarin, she was not able to read or understand these letters on her own. When Ms. L. met with a financial coach, she and the coach reviewed the letters she had received as well as her credit report and found several accounts that had been opened under Ms. L.'s name without her knowledge or permission. Ms. L. and her financial coach first attempted to contact the creditors to request that the accounts be closed and that they begin a fraud investigation. Some of the creditors accommodated this request, but others refused to close the accounts or file fraud claims until they received a police report for the identity theft. To move forward with the process, Ms. L. went to her local precinct with a completed Federal Trade Commission Identity Theft Affidavit and copies of the credit card bills to file the report. Ms. L. made three separate visits and was turned away for different reasons each time. After the last attempt, Ms. L. and her financial coach decided to submit the Identity Theft Affidavit to the creditors and credit bureaus without the law enforcement section

⁵ N.Y. Gen. Bus. Law § 380-t(n).

completed. Because this section was not completed, three of the creditors refused to release Ms. L. from these debts, leaving her, a woman unable to speak, read, or write English responsible for paying the fraudulent accounts.

Recommendations to mitigate the impacts of identity theft on the lives of New Yorkers

To improve the process of obtaining relief and removing liability after identity theft, we respectfully request that the Committee consider the following:

- *Create a special mechanism for domestic violence survivors, and identity theft victims more generally, to pull their credit reports.* For example, approved domestic violence service providers, consumer advocacy and legal services organizations, and financial counselors could serve as intermediaries to enable the verification process and permit access without divulging confidential or safe locations. Some kind of certification process by service providers would be helpful here, but should not require a court order of protection or a police report.
- *Establish a New York state form identity theft report to satisfy the law enforcement report requirement for credit reporting agencies, creditors, and the courts.* This form could be taken by or recorded with a variety of state agencies, such as the New York State Department of Financial Services or the New York State Office of the Attorney General. The ability to make a uniform report with governmental agencies in addition to local police departments would help identity theft victims collect the documentation they need to pursue relief. Because difficulty in filing identity theft reports is such a pervasive problem, we recommend the Committee hold a hearing and invite local law enforcement throughout the state to testify on their policies and practices.
- *Ban credit checks in employment statewide.* Survivors of domestic violence, along with other low-income New Yorkers, are frequently caught in a cycle of unemployment and increasing debt with no way out. Their poor credit scores prevent them from obtaining jobs, and without income, they are unable to address their debts; importantly, these credit scores for a vast majority of jobs are not meaningfully predictive of employee performance and thus do more harm than good. The credit reports of identity theft victims who have not yet obtained relief are viewed similarly to those of any other debtor, and these New Yorkers are frequently and unfairly denied employment as a result.
- *Eliminate the fees for all of the steps involved in placing, lifting, and reissuing credit freezes free for New Yorkers.* The fees related to credit freezes differ by state. Currently, the fees for lifting and reinstating a credit freeze are waived for domestic violence survivors and identity theft victims in New York. However, as explained in this testimony, these populations are not always able to obtain the documentation necessary to establish that they are entitled to the fee waiver. Making all actions related to credit freezes free for New Yorkers would allow more residents to access the remedies that they desperately need to prevent additional fraud.

We greatly appreciate your consideration of this testimony, and welcome the opportunity to further discuss these important issues.



NEW YORKERS FOR RESPONSIBLE LENDING

Testimony of New Yorkers for Responsible Lending

**NEW YORK STATE SENATE COMMITTEE ON CONSUMER PROTECTION
2017 NYS SENATE HEARING ON IDENTITY THEFT**

September 26, 2017

Thank you to Senator Carlucci and the members of the Senate Committee on Consumer Protection for holding a hearing on this important issue. We appreciate the opportunity to provide testimony based on our experience in consumer law, identity theft recovery, and economic advocacy on behalf of low-income New Yorkers throughout the state.

New Yorkers for Responsible Lending (NYRL) is a statewide coalition of more than 160 non-profit organizations that promotes economic justice as a matter of racial and community equity. NYRL members represent community development financial institutions, community-based organizations, affordable housing groups, consumer advocacy groups, advocates for seniors, legal services organizations, housing counselors, community reinvestment, fair lending, and labor groups. The NYRL coalition is committed to fighting predatory practices in the financial services industry through policy reform, education and outreach, research and direct services.

Overview of Identity Theft

Identity theft is a complex crime that can take many different forms. While large data breaches releasing the sensitive identifying information of thousands of consumers often receive the most attention, like the recent Equifax breach, roughly 1 in 7 victims reporting identity fraud in 2010 reported that they knew the perpetrator.¹

Armed with just a few critical pieces of identifying information – a victim’s name, address, date of birth, social security number, credit card number, or some combination thereof – an identity thief has an array of options. He or she can use the victim’s credit cards, open new credit cards, get an apartment, secure employment, file taxes, obtain utility service, set up a cell phone plan, buy furniture or a car on an installment payment plan, obtain cable and internet, or get an EZ-Pass. The thief may be able to access and drain the victim’s bank accounts, and may be able to view a victim’s credit report to monitor their activities.

The consequences of identity theft are time-consuming and difficult for victims to remedy. According to a 2016 survey of identity theft victims conducted by the Identity Theft Resource Center, 61.1% of identity theft victims estimated they spent over 40 hours clearing up their identity theft case.² This may be because the consequences are so wide-ranging. In addition to directly profiting from the theft by appropriating funds directly from the victim, a thief can also cause serious, lasting damage to the victim’s credit. If a thief opens a credit account – or, more often, multiple credit accounts – and fails to make payments, the account becomes listed as an adverse account on the victim’s credit report. This can eventually lead to a debt collection lawsuit in civil court; these cases are extremely challenging for unrepresented defendants, even when they do not actually owe the debt or have other legitimate defenses.

¹ PAULA PIERCE, OFFICE FOR VICTIMS OF CRIME TRAINING AND TECHNICAL ASSISTANCES CTR., IDENTITY THEFT RESOURCE PAPER 4-5 (2012), *available at* http://www.ncdsv.org/images/OVCTTAC_IdentityTheftResourcePaper_2012.pdf.

² Identity Theft: The Aftermath 2016, Identity Theft Resource Center.

Apart from litigation, the damage caused to the victim's credit has far-reaching consequences. The presence of adverse accounts can prevent a consumer from obtaining other lines of credit, including for a car or a home mortgage. And because landlords, employers outside of New York City and some within, and other types of businesses use credit screening as a method of evaluating applicants, poor credit can prevent a consumer from obtaining an apartment, a job, utilities, and more. Less obviously, each time the thief applies for credit, the creditor will run the victim's credit, resulting in a "hard inquiry," which indicates when a consumer's file has been reviewed in connection with an application for credit. Hard inquiries may bring down the consumer applicant's credit score.

Even uncovering the extent of identity theft poses significant challenges. People attempting to obtain their credit report online must typically answer security questions, which may be about past addresses or credit accounts. Victims of identity theft often do not know the details of the accounts taken out in their name, and so are unable to answer the security questions. If the victim is thereby unable to access their credit report online, they must order it by mail – which has its own problems, including that credit reporting agencies may mail the report to a prior address instead of the one requested by the consumer, which may be the address used by the thief or which may be a place the consumer no longer lives, exposing their information to further theft.

Resolving Identity Theft

The process of repairing the harm caused by identity theft is time-consuming, arduous, and frustrating. In addition to dealing with government agencies like the IRS and the Social Security Administration, consumers must aggressively pursue disputes with multiple creditors and credit reporting agencies (CRAs) – often meeting with little success.

Removing Harm to Credit: Disputes with Credit Reporting Agencies

Under the Fair Credit Reporting Act, CRAs must block accounts resulting from identity theft from individual credit reports if the consumer provides proof of identity, an "identity theft report," the details of the information requested to be blocked, and a statement by the consumer that the information does not relate to a transaction by the consumer.³ Under FCRA, victims with an identity theft report can prevent a creditor from refurnishing fraudulent information to a CRA; prevent a creditor from selling the fraudulent debt to another company or placing it with a collection agency; place an extended, seven-year fraud alert on their credit report; and require a creditor to disclose account activity made by the identity thief and provide the company's business records related to the transaction(s) in question. An identity theft report is defined as a report that alleges identity theft and that is a copy of an official report filed by a consumer with a federal, state, or local law enforcement agency, or other government agency deemed appropriate by the bureau, the filing of which subjects the person filing to criminal penalties for filing false information.

The "identity theft report" requirement poses particular challenges. On paper, such a report seems to provide access to critical remedies for victims of identity theft. But although the

³ 15 U.S.C. 1681c-2.

FCRA defines the term “identity theft report” broadly, CRAs typically strictly construe the term as referring specifically to a police report. They frequently reject requests for the block that include another type of identity theft report, such as the Federal Trade Commission’s Identity Theft Report.

Furthermore, CRAs often simply ignore disputes. The dispute process is lengthy, mostly automated, and often requires persistent and voluminous documentation, including police reports or affidavits. Multiple letters and complaints to CRAs are typically required, and sometimes even litigation. Because the CRAs do not have uniform investigation procedures, the same dispute submitted to all three major CRAs may have different results with each one.

Removing Liability: Disputes with Original Creditors or Service Providers

Removing liability with the original creditor or service provider involved in the identity theft can be even more challenging than disputing the debt or account with the CRAs. There is no uniform process for these entities to deal with fraud, and identity theft victims often spend a significant amount of time obtaining and providing different types of documentation and various affidavits and forms to support their identity theft claim. Most entities prefer victims to fill out their own forms rather than simply accepting the FTC’s identity theft affidavit and/or report.

While procedures vary widely, one frequent commonality is that creditors, providers, and the courts will typically require identity theft victims to produce a police report substantiating their claim. Under New York state law, an individual may use a valid police report as proof of identity theft in order to stop creditors from collecting on debt accrued by the identity thief; prevent creditors from denying credit, reducing credit, or increasing the cost of credit due to debts incurred by an identity thief; and waive fees for freezing the victim’s credit report, to prevent further fraud.

Obtaining Law Enforcement Reports

Unfortunately, while many states, including New York, require police departments to take these reports, in our experience many victims are unable to obtain an actual police report. Consumers may be bounced between precincts or told that theft of their information by a spouse, partner or family member is not a crime; that they cannot file a report without the name and contact information of a suspect; that they cannot file a report unless there is a court case against them; that they cannot file a report without complete account statements; and more.

These demands reflect confusion about the nature of modern identity theft. For example, it is incredibly difficult to obtain account statements or payment histories for most fraudulently created debts, particularly old ones. Victims usually do not know who committed identity theft against them, and even if they do they are unlikely to know how to contact the perpetrator. And identity theft is always a crime, even when committed by a spouse or romantic partner.

The police report is a critical tool for victims seeking relief from identity theft related debt. Without a valid report, victims of identity theft often have limited recourse against creditors or within the judicial system.

Client Stories

We offer the client stories below to exemplify how critical the proper report becomes in obtaining relief, and the current challenges our clients face in obtaining these reports.

Mr. S. was a longtime customer of an authorized cell phone retailer in Queens. In 2012, the franchise owner scammed hundreds of his own customers, including Mr. S., by fraudulently opening accounts in their names and accruing charges to their bills without their knowledge. When his fraud was discovered and reported in the news, the owner left town and was never found. At the time, Mr. S. tried repeatedly to obtain a police report and resolve the issue with the provider directly, without success. Recently, in the spring of 2017, Mr. S. resumed these efforts, visiting his local precinct twice and contacting the creditor as well. The NYPD told him the provider must file the report for them to act and the provider told him he needed a police report for them to do anything. Stuck between these directives, the debt remained on his credit report until he was able to retain an attorney to assist him.

Mr. C. first learned he was an identity theft victim in September 2015, when he was sued for breach of a car lease that he knew nothing about. When he tried to report the crime, Mr. C. was repeatedly sent back and forth between his local precinct and the Bronx precinct where the dealership that leased the car was located, with each refusing to assist and claiming that the other was the proper place to file. Confused, Mr. C. revisited his local precinct, accompanied by a law student advocate, where they were wrongly informed that Mr. C. had to provide the NYPD with a copy of his credit report before they could file an identity theft report. Mr. C.'s identity theft report was not filed until nearly one month after his first attempt and was riddled with errors. In total, Mr. C. made over eight visits to various precincts before having his report adequately filed in a form that would provide him relief from the identity theft.

Prevention of Future Identity Theft

Once a consumer learns that he or she has been a victim of identity theft, there are several options that can prevent additional identity theft. The most commonly used are fraud alerts and freezes.

An extended fraud alert adds a notation to the consumer's credit report requiring any entity reviewing it to take additional steps to verify the consumer's identity before extending credit or offering a service. These alerts last for seven years and are free to place, but require an identity theft report.

Credit freezes provide more security but are also more burdensome. They block access to a consumer's credit report entirely, thus preventing new accounts from being opened. They can be lifted on a temporary basis or for a specific creditor, upon notice to the CRAs and identification by the consumer's PIN number. In New York, initial placement of the credit freeze is free; thereafter, there is a fee every time the freeze is lifted or placed again. Fees are waived for victims of identity theft and domestic violence with the proper documentation.

As discussed in this testimony, the documentation requirement is particularly problematic for many New Yorkers. Without proper documentation, the fees can add up quickly, especially for low-income residents. Because credit checks are performed for all types of credit access as well as by landlords, utility providers, insurance companies, and cell phone providers, temporarily lifting and reinstating the credit freeze will be necessary for most individuals.

Recommendations

We respectfully offer the following recommendations for the Committee to consider:

- *Establish a New York state form identity theft report to satisfy the law enforcement report requirement for credit reporting agencies, creditors, and the courts.* This form could be taken by or recorded with a variety of state agencies, such as the Department of Financial Services or the New York Attorney General's Office. Creating a uniform report with governmental agencies outside local police departments would allow identity theft victims the documentation they need to pursue relief. The department tasked with taking the report should have reasonable, uniform, and transparent policies regarding what types of proof or documentation victims will be required to produce.
- *Create a uniform procedure for creditors, collectors, service providers, and other similar entities licensed by the state to use in responding to identity theft.* Such a process should reflect the issues raised in this testimony, and attempt to strike a fair balance between legitimizing identity theft claims without making it unduly burdensome or impossible for identity theft victims to comply.
- *Require creditors, collectors, service providers, and other similar entities licensed by the state to provide multiple confirmations of a new account opened using their information.* If consumers receive prompt, adequate notice of new accounts, they will be better positioned to address the identity theft quickly and before significant damages accrue, both for the consumer and for the entity providing the credit or service.
- *Ban credit checks in employment statewide.* Low-income New Yorkers are frequently caught in a cycle of unemployment and increasing debt with no way out. Their poor credit scores prevent them from obtaining jobs, and without income, they are unable to address their debts. The credit reports of identity theft victims who have not yet obtained relief are viewed similarly to those of any other debtor, and these New Yorkers are frequently denied employment as a result.
- *Make placing, lifting, and reissuing credit freezes free for New Yorkers.* Making all actions related to credit freezes free for New Yorkers would allow more residents to access the remedies that they desperately need to prevent additional fraud.