Protecting New Yorkers from Identity Theft

A Report of the New York State Senate Standing on Consumer Protection

Senator David Carlucci, Chair

EXECUTIVE SUMMARY

In response to the findings of this hearing, we recommend an eight-point plan to combat identity theft and protect New Yorkers from identity theft. We call on state government, and the federal government where necessary, to adopt each one of these points without delay.

1. Expanding the Definition of Private Information

We recommend the enactment of S. 6890/A. 8709 by Senator Carlucci and Assemblywoman Fahy, which expands the definition of "private information," the disclosure of which would trigger state data breach protocols to include birthdates, home addresses, and telephone numbers. It also removes the requirement that credit card, debit card, and bank account numbers be disclosed along with passwords or security codes to be considered a breach.

2. Give New York State Statutory Authority Over Credit Reporting Agencies

We recommend enacting S. 6878 by Senator Comrie, giving the New York State Department of Financial Services (DFS) licensing authority over credit reporting agencies, as well as the ability to review their records.

3. Drastically Reduce Notification Time

We recommend the enactment of S. 6891 by Senator Carlucci, requiring that a preliminary notification that a breach may have occurred be sent to the Attorney General within 24 hours and to all effected parties within 48 hours. We also recommend the enactment of S. 1104A by Senator Valesky, requiring that notification that a breach has occurred be sent to all effected parties and the Attorney General within 45 days.

4. Set Minimum Data Security Standards for All Large Companies

We recommend the reintroduction and enactment of the Data Security Act. This bill sets minimum, flexible data security standards for credit reporting agencies and other entities including reasonable data safeguards, independent audits by licensed auditors, and a safe harbor provision for those who meet heightened federal standards.

5. Making Credit Freezes Free for All Consumers

Under current law, only an initial credit freeze is free, regardless of whether a breach has occurred. However, companies can charge up to a $5 fee unfreeze or refreeze your credit. We recommend the enactment of S. 6891 by Senator Carlucci, requiring that companies offer free credit freezes and unfreezes to all New Yorkers at any time.

6. Providing Free Credit Monitoring to All New Yorkers

We recommend the enactment of S. 6912 by Senator Carlucci, requiring that companies that suffer a data breach provide free credit monitoring services to effected parties for one year following a breach.

7. Free FICO

We recommend the enactment of S. 6913 by Senator Carlucci, which would implement a public outreach program to help educate New York consumers about their rights to access their credit report under the federal Equal Credit Opportunity Act, as well as the workings of FICO scores. S. 6914, also by Senator Carlucci, implements a broader education and outreach program to inform consumers about topics such as their rights to notification of a data breach, credit freezes, and credit monitoring, among other topics. Additionally, we call on the federal government to make access to credit reports and FICO scores free in all cases, for all consumers, at any time.

8. Enact S. 5576 Allowing Consumers to "Opt-In" to Any Sharing of Their Personal Information

We recommend the enactment of S. 5576 by Senator Carlucci, requiring internet service providers to provide customers with a copy of their privacy policy and to obtain written and explicit permission from a customer prior to sharing, using, selling or providing any sensitive information to a third party.

INTRODUCTION

Identity theft is the unlawful use of an individual's personal identification information. Identity thieves steal information such as your name, social security number, driver's license information, or bank and credit card accounts and use the information to establish credit, make purchases, apply for loans or even seek employment.

Identity theft is a growing threat to consumers across the state and the country. Identity theft scams are on the rise. According to USA Today, identity theft incidence rates rose 16% between 2015 and 2016, alone. 15.4 million Americans were estimated to have been effected, a drastic increase of nearly 2 million people in a single year. That accounts for 1 in 16 adults in the United States.[1] In New York, there were 24,157 incidences of identity theft reported in 2015, the fourth highest number in the nation.[2] Additionally, the number of seniors victimized by identity thieves rose from 2.1 million in 2012 to 2.6 million in 2014.[3]

Identity theft complaints to the Federal Trade Commission (FTC) have skyrocketed over the past decade (*see exhibit A, below*).[4] Identity theft now accounts for the third most common type of complaint to the FTC.[5]

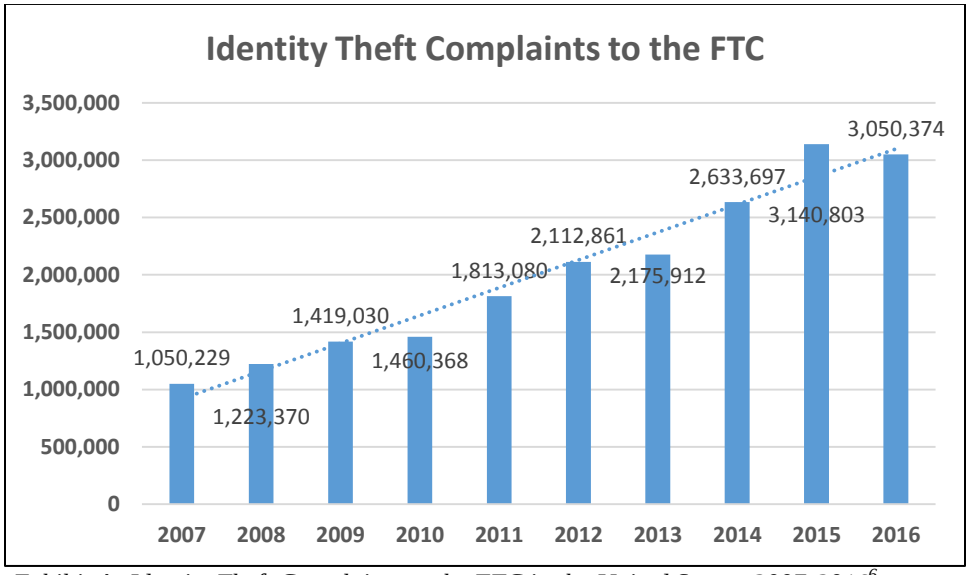

Exhibit A: Identity Theft Complaints to the FTC in the United States, 2007-2016[6]

[1] https://www.usatoday.com/story/money/personalfinance/2017/02/06/identity-theft-hit-all-time-high-2016/97398548/
[2] https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime#Identity%C2%A0theft%C2%A0and%20fraud%20complaints
[3] https://www.bjs.gov/index.cfm?ty=pbdetail&iid=5408
[4] https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime#Identity%C2%A0theft%C2%A0and%20fraud%20complaints
[5] https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime#Identity%C2%A0theft%C2%A0and%20fraud%20complaints
[6] https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime#Identity%C2%A0theft%C2%A0and%20fraud%20complaints

Identity theft cost consumers $16 billion in 2016 [7] (representing an increase of $1 billion from 2015).[8] If that trend continues at the 2016 rate, the annual cost could rise by more than $11 billion during the next decade to a total of over $27.6 billion by 2025 (*see exhibit B, below*). According to the New York State Division of Consumer Protection, identity theft is the most common consumer fraud complaint and of particular concern in New York, which has one of the highest per-capita rates of identity theft in the country.[9]

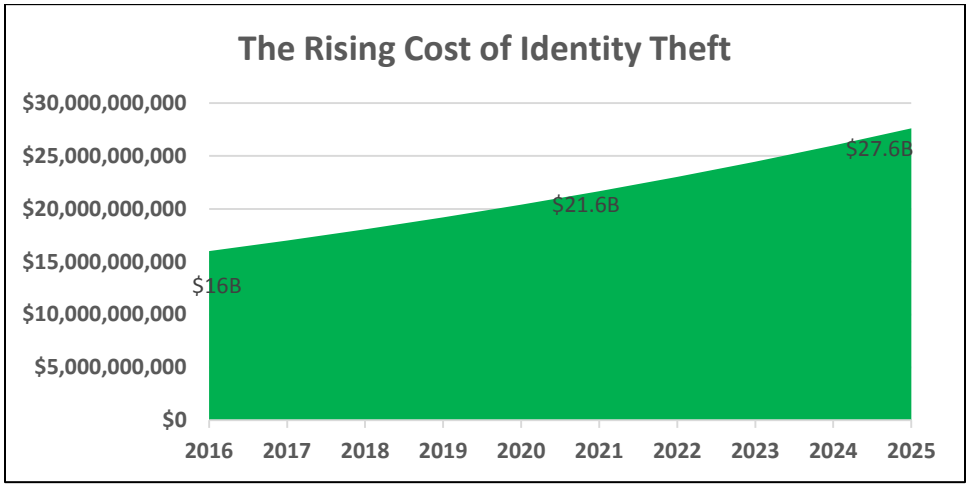

Exhibit B: Projected cost of Identity Theft Nationally Over the Next Decade, at 2016 Rate

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 are victims of identity theft.[10] Yet, this problem impacts people of all ages. A recent study by the Federal Bureau of Justice Statistics found that 7% of persons 16 years of age are older were victims of identity theft.[11] Perhaps most surprising – children aged 19 and younger represent 8% of all identity theft victims.[12] As the NYS Coalition on Elder Abuse points out, often a greater number of people have access to the personal information of vulnerable adults who are unable to restore stolen funds through employment[13].

Identity theft can deprive hardworking consumers of their livelihood. Identity theft complaints account for 13% of all FTC complaints overall.[14] About 29% of identity theft complaints to the FTC are related to tax fraud.[15] Identity theft can happen anywhere, and it most frequently does – online. According to CNBC, online and over-the phone incidences of fraud, specifically where the cardholder does not need to be present, rose most sharply between 2015 and 2016. Incidences of consumers being tricked into giving out credit card information rose 40%. Account takeover

[7] https://www.cnbc.com/2017/02/01/consumers-lost-more-than-16b-to-fraud-and-identity-theft-last-year.html
[8] https://www.nbcnews.com/business/consumer/identity-fraud-hits-record-number-americans-2016-n715756
[9] https://www.dos.ny.gov/consumerprotection/pdf/ID_Theft_Brochure.pdf
[10] https://amac.us/senior-id-theft-top-ftc-consumer-complaint/
[11] https://www.bjs.gov/index.cfm?ty=pbdetail&iid=5408
[12] https://amac.us/senior-id-theft-top-ftc-consumer-complaint/
[13] https://www.nyselderabuse.org/identity-theft/
[14] http://blog.aarp.org/2017/03/10/ftc-impostor-scams-surpass-id-theft-but-debt-collection-remains-top-complaint/
[15] http://blog.aarp.org/2017/03/10/ftc-impostor-scams-surpass-id-theft-but-debt-collection-remains-top-complaint/

fraud rose 31%. The opening of bank accounts by criminals under a consumer's name rose 20%.[16]

Identity theft is a crime under the New York State penal law. Identity theft in the first degree is a class D felony. It carries a sentence of probation or up to 3 to 7 years' jail time, fixed by the court.

HISTORY

The credit reporting industry in the United States began like so many other businesses – in a small storefront. In fact, its history can be traced back two hundred years, to the earliest days of the American Republic.[17] Back then, merchants would keep records of – or even share by word of mouth – which customers were most reliable to pay back debts owed.[18] Equifax itself grew from a storekeeper in late 19th Century Tennessee who kept a list of customers with good credit into a multibillion-dollar firm.[19]

Times have changed dramatically, of course. A person's word alone is no longer enough to establish creditworthiness. As the credit card industry grew, so did losses to credit card companies on customers who defaulted.[20] The effect was a parallel growth in the need for credit reports, information collection and the credit reporting agencies that provided these services.[21]

The first major regulation of the credit industry came in the form of the federal Fair Credit Reporting Act of 1970.[22] It was a significant step, restricting access to credit reports by limiting who can see it.[23] In 2005, this law was expanded to give consumers the right to see their credit report for free once a year. [24] [25] The law also gave consumers the right to be given their credit score (or FICO score) from credit reporting agencies, for a fee.[26] Over the years, both the federal government and New York State have passed numerous laws regulating the credit industry and protecting the rights of consumers.[27] This includes New York's Fair Credit Reporting Act (adopted in 1977 and updated numerous times, including improving its security freeze provisions in 2011) and its law defining "private information" (passed in 2005 and updated in 2013).

Despite this, more can be done. The Equifax breach proved that more *has* to be done. The problem with existing law is that it did not anticipate (or at least not adequately so) the digital, interconnected world of the Twenty-First Century. In particular, it was not prepared for the ways cyber criminals and identity thieves would leverage technology to steal private information. The figures speak for themselves. Data breaches nationally increased by 71% just between 2015 and

[16] https://www.cnbc.com/2017/02/01/consumers-lost-more-than-16b-to-fraud-and-identity-theft-last-year.html
[17] http://time.com/3961676/history-credit-scores/
[18] http://time.com/3961676/history-credit-scores/
[19] https://www.creditrepair.com/blog/credit/credit-bureau-history/
[20] https://www.creditrepair.com/blog/credit/credit-bureau-history/
[21] https://www.creditrepair.com/blog/credit/credit-bureau-history/
[22] https://www.creditcards.com/credit-card-news/history-of-credit-cards.php
[23] https://www.creditcards.com/credit-card-news/your-rights-fair_credit_reporting_act-1282.php
[24] https://www.creditcards.com/credit-card-news/your-rights-fair_credit_reporting_act-1282.php
[25] https://www.consumer.ftc.gov/topics/credit-and-loans
[26] https://www.consumer.ftc.gov/topics/credit-and-loans
[27] https://www.creditcards.com/credit-card-news/history-of-credit-cards.php

2016 [28] (*see exhibit C, on the next page* [29]). The unfortunate reality is that criminals adapt very quickly. The law – and most importantly the governments that enact and enforce it – needs to adapt even more quickly to protect the public.

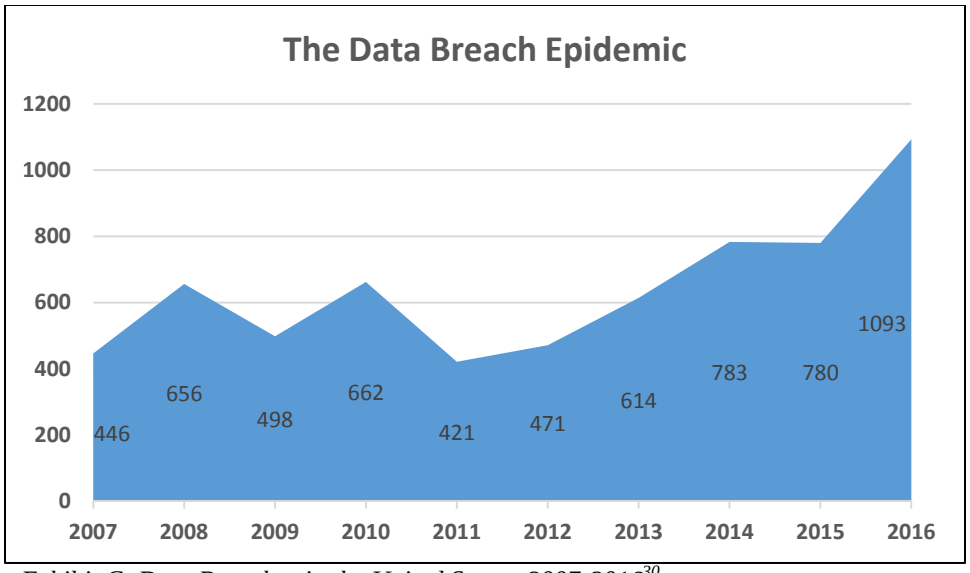

Exhibit C: Data Breaches in the United States, 2007-2016[30]

EQUIFAX

The need for action was made strikingly clear by the massive consumer data breach that effected Equifax. Equifax, along with TransUnion and Experian, is one of three major credit bureaus. The breach compromised the personal information of 145.5 million Americans (or 45% of the population). This included 8 million New Yorkers. Data compromised by the breach included social security numbers, driver's license numbers, birthdays, home addresses, and telephone numbers.

The cost of this breach was also enormous. The stock market is estimated to have lost $4 billion in value in the wake of the breach. Time Magazine estimates that it could cost Equifax as much as $300 million to mitigate the damage done. The cost to consumers – the most important cost of all – is harder to quantify, but it is safe to say it could run into the billions of dollars.

Equifax has taken some actions to mitigate what has occurred. Primarily, it has offered free credit freezes to effected customers. A credit freeze is a hold on the transfer of any of a consumer's personal information held by a credit reporting agency. Credit freezes are governed primarily by state law (as there are no firm federal rules on the subject), but there are some universal elements to them (addressed below). One of these elements is that they generally come

[28] https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime#Identity%C2%A0theft%C2%A0and%20fraud%20complaints
[29] https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime#Identity%C2%A0theft%C2%A0and%20fraud%20complaints
[30] https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime#Identity%C2%A0theft%C2%A0and%20fraud%20complaints

at the cost of a fee. Equifax only agreed to provide freezes for free after immense public pressure and even then only for 30 days.

The Equifax breach has exposed millions of Americans to the threat of identity theft, and all that comes with it. It is incumbent on government to act to ensure that the industry is doing all it can to keep customers and their information safe.

PROPOSED REGULATIONS

Governor Cuomo has proposed a list of new regulations that would address breaches like the one that effected Equifax. The regulations are to be implemented by the Department of Financial Services (DF). These regulations will:

- Require credit rating agencies to register with NYS
    - Register annually with DFS by February 1, 2018
    - Registration must include the agency's officers/directors who will be responsible for compliance with the law and regulations
- Give DFS the authority to revoke credit rating agencies ability to do business with New York State regulated financial institutions if the agency is not in compliance with NY's cyber security regulations that go into effect on April 4, 2018 (summarized at the end of this section) or are engaged in unfair, deceptive, or predatory business practices
- DFS may also refuse to renew a credit reporting agency's registration if the superintendent finds that the applicant or any member, principal, officer or director of the applicant, is not trustworthy and competent to act as or in connection with a consumer credit reporting agency, or that the agency has given cause for revocation or suspension of such registration, or has failed to comply with any minimum standard.
- Subject credit reporting agencies to examinations by DFS as often as the superintendent deems necessary
- The new regulations also prohibit:
    - Directly or indirectly employing any scheme, device or artifice to defraud or mislead a consumer.
    - Engaging in any unfair, deceptive or predatory act or practice toward any consumer or misrepresent or omit any material information in connection with the assembly, evaluation, or maintenance of a credit report for a consumer located in New York State.
    - Engaging in any unfair, deceptive, or abusive act or practice in violation of section 1036 of the Dodd-Frank Wall Street Reform and Consumer Protection Act.
    - Including inaccurate information in any consumer report relating to a consumer located in New York State.
    - Refusing to communicate with an authorized representative of a consumer located in New York State who provides a written authorization signed by the consumer, provided that the consumer credit reporting agency may adopt procedures reasonably related to verifying that the representative is in fact authorized to act on behalf of the consumer.

- Making any false statement or make any omission of a material fact in connection with any information or reports filed with a governmental agency or in connection with any investigation conducted by the superintendent or another governmental agency.

The Governor through DFS has implemented new cyber security regulations. As noted above, credit reporting bureaus would now have to comply with these as well. The new regulations require banks, insurance companies, and other financial institutions regulated by the DFS to adopt certain cybersecurity measures and standards. Firms would be required to designate a chief information officer and to adopt a written cybersecurity policy. The policy would address information security, customer data privacy, vendor and third-party service provider management, and business continuity planning, among other things. Firms would also be required to implement minimum standards and procedures that third-party service providers and vendors would be required to abide by if they will be accessing confidential data. Institutions would be also required to establish a cybersecurity plan to protect consumer data. The plan would include procedures for identifying threats, responding to them, and recovering from an attack. Additionally, any cybersecurity plan would have to provide for annual penetration testing and risk assessments to determine the vulnerability of networks.

FINDINGS

This hearing generated broad interest and testimony from many different stakeholders, including government entities, industry, and public interest groups. These brought diverse perspectives to the table, but certain common themes were prevalent. These common themes are at the center of what must be done to better address identity theft and data breaches. At the center of all of this is the notion that we must put power over personal information back in the hands of the consumer.

This hearing made abundantly clear that the federal government is not doing nearly enough to regulate credit reporting agencies. While the pending federal actions noted above are commendable, concrete action is badly needed if another Equifax-style breach is to be prevented. The upshot is that the lack of federal oversight gives state government's broad discretion to implement policy solutions on their own. It is incumbent on New York State to step up to the plate to, as Superintendent Vullo put it, "fill the federal void" and protect consumers from data thieves and hackers.

One major theme of the testimony submitted was that the laws governing regulation of credit reporting agencies and data security are weak and outdated. Both the executive and legislative branches have roles to play and both can do much more to safeguard New Yorkers from identity thieves and hackers. As noted above, both state agencies such as and legislators have already taken some action in this regard, both prior to and in the wake of the Equifax data breach. However, there is more to be done and the time for action is now. Many of the same recommendations were made consistently throughout the hearing.

First, New York must upgrade its definition of private information to adapt it to changing technology. This would be a key step in bringing data security into the Twenty-First Century. This includes adding data such as birthdays, addresses, and telephone numbers to the definition

of private information under state law. It also includes removing the archaic requirement that passwords be disclosed at the same time as credit card, debit card, and bank account numbers to constitute a breach. Additionally, online account information (such as Google or Apple account passwords and search history) should be included in the definition of personal data. The definition should also be expanded to include health care information such as medical records and biometric data, as proposed in the Data Security Act.

Second, statutorily mandated oversight of credit reporting agencies by the state of New York is badly needed. While DFS has proposed several key regulations that would impact credit rating agencies, it is up to the legislature to enact a construct that would provide true oversight. For instance, as Superintendent Vullo recommended, it would take an act of the legislature to grant DFS licensing power over credit reporting agencies.

Third, breach notification requirements are woefully inadequate. DFS action in mandating that companies must inform it of a breach within 72 hours is a very good first step. However, consumers, the Attorney General, and other agencies can still be kept in the dark during the critical period immediately following a breach under New York's current laws. We must avoid situations where government and the public only learn of a breach months after it happened, as was the case with Equifax.

Fourth, companies must be held to minimum data security standards, set in state statute. DFS is to be commended for proposing the requirement that credit reporting agencies to adhere to the Governor's recently implemented cyber security standards. As always, more can be done and the legislature must take action to set additional requirements for data security protocols. This includes instituting a flexible security standard that takes into account the size of firms, as opposed to an ineffective "one size fits all approach." In this same vein, this standard should apply to all companies, especially large ones, and not just to health care and financial services firms.

Fifth, credit reports, credit monitoring services and credit freezes must be made freely available to all and must be available at any time, regardless of whether or not a breach has already occurred. Too often, these services are only made available when it is already too late and there is nothing left to do except mitigate the effects of a crime that has already occurred. Consumers should have open access to these services before they have already been victimized.

Sixth, consumers must have the final say over who is accessing their personal information. This is true across the board whether it is credit information, financial history, or online account data.

Seventh, New York's laws in nearly all the areas noted above are weak and ineffective in terms of punishing those who do not implement adequate data security. Throughout this hearing, it was stated that the law must be stronger in terms of penalties. At the same time, government must work cooperatively with industry to ensure best practices are being developed, implemented, and adhered to, those who are not in compliance must be held to account. At the end of the day, the goal should be to incentivize compliance. We want to make it in industry's best interests to develop and implement best practices aimed at protecting consumers, without reducing the incentive to do business in New York.

Finally, consumer education is key, especially for those already impacted by the Equifax breach. DFS has undertaken a public outreach program to help consumers effected by the breach, and this too is commendable. Government must ensure, however, that consumers are informed of their rights, how to secure their data, and what to do should that data be compromised before a breach ever occurs.

With regard to all of these issues, it is time to be proactive and not reactive. In that vein, we recommend several critical pieces of legislation that should be quickly enacted during the upcoming legislative session to protect consumers from data breaches and identity theft.

POLICY RECOMMENDATIONS

In response to the findings of this hearing, we recommend an eight-point plan to combat identity theft and protect New Yorkers from identity theft. We call on state government, and the federal government where necessary, to adopt each one of these points without delay.

1. Enact Legislation Expanding the Definition of Private Information

Current NYS law defines a breach as a bad faith unauthorized access to personal information that is contained in a computer system. Personal information is defined as social security numbers, driver's license or state ID card numbers, and credit card, debit card, or bank account numbers when leaked along with a password or security code that would give access to an individual's account.

Senator Carlucci and Assemblymember Patricia Fahy have already introduced a bill (S. 6890/A. 8709 of 2017) that expands the definition of personal information by:

- Adding in birthdays, home addresses, and telephone numbers (all of which were leaked in the Equifax breach).
- Removing the requirement that credit card, debit card, and bank account numbers must be accompanied by a password to be considered personal information that would trigger a breach. Under this bill, merely leaking the numbers would be sufficient.

Additionally, this bill will soon be amended to add medical information of any kind to the list of data considered personal information.

At the same time, we recommend the reintroduction and enactment of the Data Security Act. This legislation takes a comprehensive approach to data security, including the critical step of adding biometric information to the definition of private information.

2. Enact Legislation Giving New York State Statutory Authority Over Credit Reporting Agencies

We recommend that the legislature give New York State the power to license credit reporting agencies to do business in the state of New York. The bill should require that credit reporting

agencies apply to the state for a license to operate as a credit reporting agency. It should also give the state oversight authority, such as the ability to audit data protection procedures of credit reporting agencies. Finally, the bill should include penalties for non-compliance, in particular empowering the superintendent to revoke an agency's license to do business in the state for failure to comply.

To that end, we recommend the enactment of S. 6878 of 2017 by Senator Comrie. This bill accomplishes these objectives. It also includes empowering DFS to examine the books and records of credit reporting agencies in order to ensure compliance with the provisions of this bill and any regulations promulgated by DFS under it.

3. Drastically Reduce Notification Time

Current state law requires notice be given to New Yorkers effected by the breach "whose private information was, or is reasonably believed to have been, acquired by a person without valid authorization." Such notice must include:

- Contact info for the company that was breached and
- A description of any information believed to have been leaked

In short – companies do not have to do very much to make consumers whole. The notice has to "be made in the most expedient time possible and without unreasonable delay." However, this can be delayed if there is an ongoing law enforcement investigation (the law enforcement agency determines if there is a delay) or to allow for "any measures necessary to determine the scope of the breach and restore the reasonable integrity of the system" to be taken.

Senator Carlucci has introduced a bill (S. 6891 of 2017) that would require preliminary notice that a breach may have occurred be sent to the Attorney General within twenty-four hours after the discovery of the breach. Senator Carlucci's bill also requires that preliminary notice that a breach may have occurred be sent to any resident of New York State believed to have been affected by the breach within forty-eight hours after the breach's discovery. We recommend the enactment of this legislation.

We also recommend the enactment of a bill by Senator Valesky (S. 1104-A of 2017) that would require companies issue definitive notification that personal information has been breached to any effected consumers within forty-five days of discovery that a breach has occurred.

4. Enact Legislation Setting Minimum Data Security Standards for All Large Companies

We recommend statutorily set data security minimums built on a flexible standard and applied to all companies over a certain size. This means expanding current laws to cover firms beyond just those in the health care and financial services fields. It also means updating the standard to improve its flexibility and protect small businesses.

The Data Security Act sets out a standard that fulfills these criteria. Once again, we recommend its reintroduction. The standard laid out in the Data Security Act is both comprehensive and considers the needs of all stakeholders, including private industry.

The Data Security Act lays out a comprehensive, balanced standard that includes:

- Reasonable data security requirements for entities conducting business in the State of New York that own or license private information. These must develop, implement, and maintain reasonable safeguards to protect the security, integrity, and confidentiality of any private information they possess.
- Authorizing DFS to allow independent, third party, licensed insurers to conduct audits of regulated entities and to certify that the entity has met the reasonable data security standard.
- A rebuttable presumption that businesses that are certified through annual audits by independent, third party, licensed insurers are maintaining reasonable data security safeguards.
- A safe harbor provision which removes liability to both the Attorney General and consumers effected by a data breach for entities that comply with the heightened federal data security standard put in place by the US Department of Commerce. In order to qualify for the safe harbor provision, compliance must be annually assessed by an independent, federally accredited licensed assessment organization.

The Data Security Act also includes penalties for non-compliance with this standard, including empowering the Attorney General to seek injunctions and money damages for losses incurred in a data breach. These include up to $250 in damages per person effected by a breach, capped at 410 million.

This standard is both equitable and flexible. Once again, we recommend the swift reintroduction and enactment of the Data Security Act in order to implement this standard.

5. Make Credit Freezes Free for All Consumers

Current state law requires an initial credit freeze be available for free to all consumers (even if a breach has not occurred. A subsequent "thaw" and refreezing the same information will individually cost consumers a fee of $5. This may sound like a nominal cost, but it can add up quickly.

All three major credit bureaus offer credit freezes, usually for around $10 nationwide. The cap is $5 in New York State. In New York, the first freeze is free, but thawing and refreezing cost $5. The issue is that (a) consumers must pay the fee every time they thaw their credit and every time they refreeze it. What is more costly is that consumers must request a credit freeze with all three credit bureaus separately to truly protect their data.

Applying the New York cost, this means most credit thaws will cost a New Yorkers $15 to thaw and $15 to refreeze (a total of $30). That figure is about $60 nationwide (and $90 in states where the first freeze is not free, which it is not in many).

Some New Yorkers are entitled to free credit thaws and refreezes, specifically victims of identification theft and domestic violence. However, the fees will only be waived if the person requesting a waiver provides very personal information to the credit reporting agency as proof. In order to obtain a credit freeze fee waiver, victims of identity theft must submit to the credit agency:

- a copy of a signed federal trade commission ID theft victim's affidavit, or
- a report of ID theft from a law enforcement agency to such consumer credit reporting agency

While, victims of domestic violence must submit to the credit agency:

- a valid domestic violence incident report form; or
- a valid police report; or
- a valid order of protection; or
- a signed affidavit from a licensed medical or mental health care provider, employee of a court acting within the scope of his or her employment, social worker, a rape crisis counselor, or advocate acting on behalf of an agency that assists domestic violence victims.

We recommend that enactment of legislation introduced by Senator Carlucci (S. 6891 of 2017) that makes all credit freezes free for life and addresses other inequities. This bill:

- Requires credit reporting agencies to provide free lifetime credit freezes, thaws, and refreezes to all consumers, whether or not a breach has occurred
- Reduces the period of time it takes to implement a credit thaw from three business days to one business day
- Removes burdensome proof requirements for victims of identification theft and domestic violence
- Expands current New York State credit freeze laws to cover all credit information-related businesses

6. Providing Free Credit Monitoring to All New Yorkers

Under current state law, consumers are not entitled to free credit monitoring. Credit monitoring is a critical way to protect personal information, but can cost as high as $120 a year. In 2014, California became the first state in the nation to require companies to provide free credit monitoring to consumers effected by a data breach. Under the California law, these companies must provide this critical service for up to one year. It is time to bring the same standard to New York.

Senator Carlucci has introduced a bill (S. 6912 of 2017) that will:

- Require any business that experiences a data breach to provide credit monitoring to effected consumers

- Require credit monitoring be covered in this manner for up to one year following a breach

We recommend the enactment of this legislation.

7. Make access to FICO Scores Free For All Consumers

One area where the federal government has taken action with regard to consumer credit information is access to credit reports and credit scores (commonly called FICO scores). State action in this area is thus largely limited by federal preemption. The federal Equal Credit Opportunity Act gives consumers the right to access their credit score free of charge:

- Once every year
- If they have been denied credit in the previous 60 days
- If they have been denied employment or insurance in the previous 60 days
- If they suspect someone has been fraudulently using your accounts or your identity
- If they are unemployed and plan on applying for employment within the next 60 days
- If they are on public assistance
- They are also entitled to get their credit score free of charge from a lender when applying for a mortgage

This does not go nearly far enough. As this hearing demonstrated, frequent monitoring of one's credit report is one of the best ways to detect identity theft early. Burdening consumers with costly fees and limiting their right of access to only a select set of circumstances makes it difficult to be proactive. This in turn makes it difficult to detect a breach when one occurs. We call upon Congress and President Trump to enact quickly legislation giving consumers free access to their credit report on demand – regardless of the circumstances.

Inseparably intertwined with credit reports are credit scores. Credit or FICO scores are a number calculated based on a consumer's credit report. Credit reporting agencies calculate the score (all do so a bit differently, but the numbers are generally fairly close together) based on a credit report. They then deliver the score and the report to a lender seeking to determine creditworthiness.

FICO scores are a particularly troubling aspect of credit reporting. While they take into consideration valid factors, such as payment history and one's outstanding credit balance, they also take into account how many times a lender requests a copy of a consumer's credit report or the score itself. This is patently unfair. On its website, DFS points out that frequent requests for these may be made when one is simply in the market to buy a car. We call on Congress and President Trump to address this inequitable method by prohibiting credit reporting agencies from taking this factor into account when calculating a FICO score.

At the same time, state government must use all the power available to it to inform consumers of their rights. This will go a long way toward empowering consumers to exercise best practices when it comes to their credit. By way of example, there are common misconceptions about credit scores and reports. In particular, there is a popular belief that the amount of times the consumer

themselves requests a copy of their credit report or their FICO score can negatively impact their credit. This is simply not true, so long as the report or score is being requested directly from the credit reporting agency. Consumers should have easy access to information related to how credit reports and FICO scores do and do not impact their credit.

To that end, we recommend legislation instructing DFS to add information on obtaining and the importance of monitoring one's credit report to its existing consumer education programs. It should specifically address the rights of consumers under the federal Equal Credit Opportunity Act, including the right to obtain a free copy of one's credit report and how FICO scores can effect credit. This program should include both mailers and a television and radio campaign informing New Yorkers to contact DFS regarding their rights in this area.

Senator Carlucci has introduced a bill (S. 6913 of 2017) to make this educational outreach a reality. This bill should be enacted and the program implemented by DFS as soon as possible following its passage.

As noted above, education on the rights of consumers is critical across the board. Therefore, Senator Carlucci has also introduced legislation to establish a New York State Consumer Credit Rights and Responsibilities Outreach Program (S. 6914 of 2017). This bill directs DFS to establish and implement a comprehensive public outreach and education program. Its aim will be to educate New York consumers on what they can do to protect their personal data, track their credit information, and mitigate the impact of a data breach. The program will include, among other things, information on freezing and thawing credit, credit monitoring services, and their right to be notified promptly when their data has been compromised by a data breach.

8. Allow Consumers to "Opt-In" to Any Sharing of Their Personal Information

Consumers should have control over who can and cannot use their data. What makes the Equifax breach particularly striking is the fact that over one-half of the adult population of the United States, including 8 million New Yorkers, woke up to discover that their personal information had been breached when they never agreed to hand that data over to Equifax in the first place. In fact, it is safe to assume many people have never even heard of Equifax, TransUnion, or Experian prior to this incident. This points up the importance of putting control over data back in the hands of the consumer.

To this end, we recommend the enactment of legislation by Senator Carlucci that requires internet service providers to provide New Yorkers with a copy of their privacy policy (S. 5576 of 2017). This bill also requires internet service providers obtain written and explicit permission from a customer prior to sharing, using, selling or providing to a third party. In a world where so much of our lives happen online, this bill will go a long way toward giving consumers power over who can use their data.

Additionally, we recommend that legislation be introduced applying this same standard to other businesses including credit reporting agencies. Consumers have a right to know that firms like Equifax are in possession of their data – and right to tell Equifax to put a freeze on its usage. The

best way to give consumers the power to freeze their credit information is to know who has it in the first place.

On a larger scale, we once again call on Congress and President Trump to require that online portals such as email services, search engines, and social media platforms adopt similar standards. This includes a requirement that these websites support an "opt out button" – a setting that will allow consumers to easily control with whom who host sites can share their data.

Incentivizing Compliance

One common thread echoed repeatedly throughout this hearing, it was that current law is far too lenient on those who do not maintain adequate data security standards. This has to change and it has to change quickly. To be sure, any penalties must be reasonable. It is easy to forget that companies that are breached have also been victimized by hackers. The goal here should be to incentivize the adoption of data security best practices and compliance with state law - not to punish firms simply because they were breached.

To that end, we recommend that all of the proposed legislation noted above adopt both criminal and civil penalties for firms that are found not to be in compliance with the law and with industry standards. Though civil penalties should apply after a breach has occurred and consumer data has been compromised, criminal penalties should not necessarily be dependent on whether or not a breach has occurred. Once again, the goal is compliance, not punishment.

As noted above, it is critical that one of these penalties be the ability of the Superintendent of DFS to revoke a credit reporting agency's license to do business in the State of New York. Additionally, we reiterate that the Attorney General should have broader authority to seek civil penalties against those found to not be in compliance with applicable standards. To that end, we once again recommend the reintroduction and enactment of the Data Security Act, which accomplishes many of these goals.

Conclusion

The Equifax breach marks a watershed moment in the development of consumer protection law and policy. It has put into stark relief the changing nature of data security in the internet age. No longer will padlocks and bank vaults alone keep the American people safe from identity and data theft. Hackers across the world can attain our most private, personal information with the click of a mouse or the push of a key.

It is thus incumbent upon both government and the private sector to safeguard this private information and, more importantly, the people and families it represents. People are more than social security numbers and credit card statements – and that is the crux of the problem. Companies like Equifax need to recognize this. Every time they receive a bank code or account number, they are holding something precious in their hands. They are in possession of peoples' livelihoods – their hopes for homeownership or a college education for their kids. They hold in their hands the financial futures of their customers. Like anything precious, this must be treated with care.

The people who recognize this most are consumers themselves. They are the ones with the greatest stake in their own future. That is why to best safeguard it, the future must be put back in good hands – the hands of the consumer. We will fight to give back to the consumer the power over their own future. That is what we intend to do and that is our promise to the people of New York.