



OFFICE OF THE ATTORNEY GENERAL
STATE OF ILLINOIS

KWAME RAOUL
ATTORNEY GENERAL

December 23, 2019

RE: Social Security Number Protection Task Force
Member/Designated Recipient

Dear Designated Task Force Report Recipient,

In accordance with 20 ILCS 4040/10, attached for your review is a copy of the Social Security Number Protection Task Force Report for 2019.

Thank you.

Best Regards,

A handwritten signature in dark ink that reads "Matthew W. Van Hise".

Matthew W. Van Hise, CIPP/US
Chief, Privacy Unit
Task Force Chair
Assistant Attorney General
Consumer Fraud Bureau
Illinois Attorney General's Office

Enclosure: 2019 Task Force Report

Social Security Number Protection Task Force

Report to Governor J.B. Pritzker, Attorney General Kwame Raoul,
Secretary of State Jesse White, and Illinois General Assembly
December 23, 2019

CONTENTS

- I. Task Force Background
 - Membership of the Task Force
- II. Part I: Protection of SSNs in the Public Record
 - Identity Protection Act: Identity-Protection Policy
 - Equifax Global Settlement
- III. Part II: SSNs as Internal Identifiers
 - Minimizing the Use of Social Security Numbers
- IV. Task Force Appointments & Updates
- V. Conclusion
- VI. Appendix A: Template Identity-Protection Policy
- VII. Appendix B: Template Statement of Purpose(s)
- VIII. Appendix C: Raoul Leads 50 AGs in Largest Data Breach Settlement in History...
- IX. Appendix D: Raoul Leads 50 AGs in Largest Data Breach Settlement in History...

TASK FORCE BACKGROUND

The Social Security Number (SSN) remains the key piece of sensitive personally identifiable information that identity thieves use to commit fraud. The SSN was intended to be used solely to distribute Social Security benefits, but in the years since its inception in 1935, it has been also used as a unique identification number. The SSN is therefore not only tied to an individual's credit report, financial records, and Social Security earnings with the federal government, but is also present in employment, educational, health, insurance, and criminal records. The wide dissemination of SSNs increases the likelihood that the numbers can be accessed and subsequently used for fraudulent purposes.

Consumers are therefore encouraged to limit their exposure to identity theft by protecting their SSNs. Businesses are also encouraged to do their part by taking necessary steps to limit the collection of SSNs, protect SSNs in their possession, and dispose of documents containing SSNs in a manner that renders them unusable. Local and state government agencies also have a role in protecting SSNs they maintain and reducing their continued widespread dissemination. Government agencies have the larger task of maintaining a system of open records for the public, while taking measures to reduce the amount of sensitive personally identifiable information in those records.

The General Assembly created the Social Security Number Protection Task Force (Task Force) through Public Act 93-0813 in 2004. The Task Force is charged with examining the procedures used by the State to protect an individual against the unauthorized disclosure of his or her SSN when the State requires the individual to provide that number to an officer or agency of the State. The Task Force also is required to explore the technical and procedural changes that are necessary to implement a unique identification system to replace the use of SSNs by State and local governments for identification and record-keeping purposes. In 2007, the General Assembly amended the law governing the Task Force by Public Act 95-0482. The Office of the Attorney General is charged with chairing and administering the activities of the Task Force.

MEMBERSHIP OF THE TASK FORCE –

- Two members representing the House of Representatives, appointed by the Speaker of the House – **Representative Sara Feigenholtz, Representative Ann Williams**
- Two members representing the House of Representatives, appointed by the Minority Leader of the House – **Representative Dan Ugaste, Representative Randy Frese**
- Two members representing the Senate, appointed by the President of the Senate – **Senator Jacqueline Collins, *Awaiting Additional Member Appointment Confirmation***
- Two members representing the Senate, appointed by the Minority Leader of the Senate - ***Awaiting Additional Member Appointment Confirmation, Awaiting Additional Member Appointment Confirmation***
- One member representing the Office of the Attorney General – **Matthew W. Van Hise, Task Force Chair**
- One member representing the Office of the Secretary of State – **Micah Miller**

- One member representing the Office of the Governor – *Awaiting Member Appointment Confirmation*
- One member representing the Department of Natural Resources – **John “J.J.” Pohlman**
- One member representing the Department of Healthcare and Family Services – **Elizabeth Festa**
- One member representing the Department of Revenue – **Angela Hamilton**
- One member representing the Department of State Police – **Captain Steve Lyddon**
- One member representing the Department of Employment Security – **Joseph Mueller**
- One member representing the Illinois Courts – **James Morphew**
- One member representing the Department on Aging – **Russ Kemple**
- One member representing Central Management Services – **Tim McDevitt**
- One member appointed by the Executive Director of the Board of Higher Education – **Dr. Eric Lichtenberger**
- One member appointed by the Secretary of Human Services – *Awaiting Member Appointment Confirmation*
- Three members representing local-governmental organizations – **Dorothy Brown, Larry Reinhardt, Virginia Hayden**
- One member representing the Office of the State Comptroller – **Ben Haley**
- One member representing school administrators, appointed by the State Superintendent of Education – **Sara Boucek**

PART I: PROTECTION OF SSNs IN THE PUBLIC RECORD

The first statutory requirement of the Social Security Number Protection Task Force Act is to examine the procedures used by the State to protect an individual against the unauthorized disclosure of his or her SSN.

IDENTITY PROTECTION ACT

One way to limit the unauthorized disclosure of SSNs is to limit their collection in the first place. If fewer entities collect and use SSNs, fewer entities are capable of disclosing those numbers improperly.

The Identity Protection Act, 5 ILCS 179/1 *et seq.*, prohibits certain collections, uses and disclosures of an individual’s SSN by any person, or State or local government agencies. Specifically, the Act, with several exceptions, prohibits a person, or State or local government agency from collecting, using, or disclosing a SSN unless: (1) required to do so under state or federal law or the collection, use, or disclosure of the Social Security number is otherwise necessary for the performance of the agency’s duties and responsibilities; (2) the need and purpose for the SSN is documented before the request; and (3) the SSN collected is relevant to the documented need and purpose. The need and purpose for the collection and use of SSNs must be documented in a written Identity-Protection Policy.

Each local government agency must file a written copy of its policy with the governing board of the unit of local government within 30 days after approval of the policy. Under Section 37(b),

“each State agency must provide a copy of its identity-protection policy to the Social Security Number Protection Task Force within 30 days after the approval of the policy.” State agencies were reminded of this requirement on August 24, 2011. Policies can be submitted to the Task Force by mailing a copy to:

Illinois Attorney General
Social Security Number Protection Task Force
c/o: AAG Matthew W. Van Hise
500 S. Second Street
Springfield, IL 62706

As part of the implementation of the policies, local and state agencies will require that all employees identified as having access to SSNs in the course of performing their duties be trained to protect the confidentiality of SSNs. Training should include instructions on the proper handling of information that contains SSNs from the time of the collection of the information through its destruction.

Identity-Protection Policies were to have been implemented within 12 months of the date of approval and a copy was to have been sent to the Task Force no later than June 1, 2012. For reference, an Identity-Protection Policy and Statement of Purpose(s) template can be found in Appendixes A and B.

Updated and/or amended Identity-Protection Policies may be sent electronically to S3@atg.state.il.us. Submissions shall occur as soon as practicable or within the calendar year in which the updated amendment was implemented. An acknowledgement of receipt and record will be provided by a duly authorized representative of the Task Force chairperson.

(Template Identity-Protection Policy – Appendix A)
(Template Statement of Purpose(s) – Appendix B)

EQUIFAX GLOBAL SETTLEMENT

On July 22, 2019, Equifax Inc. entered into a global settlement (“the settlement”) with a coalition of 50 Attorneys General, the Federal Trade Commission, and the Consumer Financial Protection Bureau. The Office of the Illinois Attorney General led 50 states and territories in investigating a 2017 data breach of the credit reporting agency that affected approximately 147 million Americans. As a credit reporting agency, Equifax’s business model is inextricably intertwined with the collection and use of individual’s personal information. Equifax’s failure to maintain a reasonable security system enabled hackers to penetrate its systems, exposing the data of 56 percent of American adults and making it the largest-ever breach of consumer data. Breached information included Social Security numbers, names, dates of birth, addresses, credit card numbers, and, in some cases, driver’s license numbers.

In addition to providing direct relief to consumers, the settlement requires Equifax to make substantial changes to its security practices. The investigation found that the breach occurred

because Equifax failed to implement an adequate security program to protect consumers' highly sensitive personal information. Due to the settlement, Equifax must now create a comprehensive and rigorous information security program. The company's board of directors is required to oversee, review, and certify compliance with the program. In addition, Equifax is required to ensure regular reporting to the Board of Directors about Equifax's security posture.

Equifax also agreed to other specific terms, such as developing policies to ensure that critical updates and patches are installed in a timely manner and performing regular security monitoring, logging, and testing of its systems.

This settlement also imposes requirements on Equifax to regularly engage in penetration testing, also known as a pen test. This means that Equifax will have to regularly run simulated exercises to test its ability to respond to a security event. An additional technical safeguard and control requirement includes Equifax reorganizing and segmenting its network.

Furthermore, Equifax has agreed to employ improved access control and account management tools. This includes adopting two-factor authentication and password rotation policies. Also, it is now mandatory for the company to encrypt personal information stored on their system or adopting similar control mechanisms.

(Raoul Leads 50 AGs in Largest Data Breach Settlement in History... – Appendix C)

PART II: SSNs AS INTERNAL IDENTIFIERS

The second requirement of the Task Force is to explore the technical and procedural changes that are necessary to implement a unique identification system to replace the use of SSNs for identification and record-keeping purposes by State and local governments. State and local government agencies continue to internally assess the collection and use of SSNs. Such an assessment was critical in drafting Identity-Protection Policies.

MINIMIZING THE USE OF SOCIAL SECURITY NUMBERS

Social security numbers have become both an identifier and an authenticator. Partly due to the proliferation of data breaches exposing consumer SSNs, minimizing use of SSNs has become increasingly important. In regards to SSN minimization, the Equifax settlement was a concerted effort to limit the reliance of SSNs as authenticators by that company. The settlement requires Equifax to participate in an external organization or working group focused on the development and implementation of alternative means of identity authentication. The goal is to identify options for minimizing its use of SSNs for identity authentication purposes.

The settlement also prohibits the use of Social Security numbers as a sole authenticator by Equifax, and places other limits their use.

Furthermore, Equifax is required to minimize its collection of consumers' Social Security numbers and other sensitive data. The settlement also calls for an internal study into the primary instances in which SSNs are collected, maintained, or used by Equifax, and to evaluate potential

alternatives to such collection, maintenance, or use. The study will be provided to the CEO of Equifax, who shall establish a working group to implement identified alternatives, where feasible.

(Raoul Leads 50 AGs in Largest Data Breach Settlement in History... – Appendix D)

TASK FORCE APPOINTMENTS & UPDATES

The Task Force received the following appointment and confirmations for calendar year 2020:

The Task Force awaits calendar year 2020 Appointment and Confirmations for the following currently vacant membership seats:

- One of the two members representing the Senate, appointed by the President of the Senate
- Two of the two members representing the Senate, appointed by the Minority Leader of the Senate
- One member representing the Office of the Governor
- One member appointed by the Secretary of Human Services

CONCLUSION

Identity-Protection Policies at local and state government agencies throughout Illinois continue to be implemented according to the requirements of the Identity Protection Act. Over the course of the last year the Task Force has continued to monitor state-level discussions regarding further contemplated protections for Illinois individuals' Social Security numbers, and has also monitored federal bills involving the protections and restrictions associated with using Social Security numbers as individual identifiers. The Task Force will continue to monitor state and federal activities, recommending updates as needed and will continue to work together with all stakeholders to identify the best ways to protect SSNs in public records and limit the use of SSNs as internal identifiers.

APPENDIX A – Template Identity-Protection Policy

[AGENCY] IDENTITY-PROTECTION POLICY

The [AGENCY] adopts this Identity-Protection Policy pursuant to the Identity Protection Act. 5 ILCS 179/1 *et seq.* The Identity Protection Act requires each local and State government agency to draft, approve, and implement an Identity-Protection Policy to ensure the confidentiality and integrity of Social Security numbers agencies collect, maintain, and use. It is important to safeguard Social Security numbers (SSNs) against unauthorized access because SSNs can be used to facilitate identity theft. One way to better protect SSNs is to limit the widespread dissemination of those numbers. The Identity Protection Act was passed in part to require local and State government agencies to assess their personal information collection practices, and make necessary changes to those practices to ensure confidentiality.

Social Security Number Protections Pursuant to Law

Whenever an individual is asked to provide this Office with a SSN, [AGENCY] shall provide that individual with a statement of the purpose or purposes for which the [AGENCY] is collecting and using the Social Security number. The [AGENCY] shall also provide the statement of purpose upon request. That Statement of Purpose is attached to this Policy.

The [AGENCY] shall not:

- 1) Publicly post or publicly display in any manner an individual's Social Security number. "Publicly post" or "publicly display" means to intentionally communicate or otherwise intentionally make available to the general public.
- 2) Print an individual's Social Security number on any card required for the individual to access products or services provided by the person or entity.
- 3) Require an individual to transmit a Social Security number over the Internet, unless the connection is secure or the Social Security number is encrypted.
- 4) Print an individual's Social Security number on any materials that are mailed to the individual, through the U.S. Postal Service, any private mail service, electronic mail, or any similar method of delivery, unless State or federal law requires the Social Security number to be on the document to be mailed. SSNs may be included in applications and forms sent by mail, including, but not limited to, any material mailed in connection with the administration of the Unemployment Insurance Act, any material mailed in connection with any tax administered by the Department of Revenue, and documents sent as part of an application or enrollment process or to establish, amend, or terminate an account, contract, or policy or to confirm the accuracy of the Social Security number. A Social Security number that is permissibly mailed will not be printed, in whole or in part, on a postcard or other mailer that does not require an envelope or be visible on an envelope without the envelope having been opened.

In addition, the [AGENCY] shall not¹:

¹ These prohibitions do not apply in the following circumstances:

(1) The disclosure of Social Security numbers to agents, employees, contractors, or subcontractors of a governmental entity or disclosure by a governmental entity to another governmental entity or its agents, employees, contractors, or subcontractors if disclosure is necessary in order for the entity to perform its duties and

- 1) Collect, use, or disclose a Social Security number from an individual, unless:
 - i. required to do so under State or federal law, rules, or regulations, or the collection, use, or disclosure of the Social Security number is otherwise necessary for the performance of the [AGENCY]'s duties and responsibilities;
 - ii. the need and purpose for the Social Security number is documented before collection of the Social Security number; and
 - iii. the Social Security number collected is relevant to the documented need and purpose.
- 2) Require an individual to use his or her Social Security number to access an Internet website.
- 3) Use the Social Security number for any purpose other than the purpose for which it was collected.

Requirement to Redact Social Security Numbers

The [AGENCY] shall comply with the provisions of any other State law with respect to allowing the public inspection and copying of information or documents containing all or any portion of an individual's Social Security number. The [AGENCY] shall redact social security numbers from the information or documents before allowing the public inspection or copying of the information or documents.

When collecting Social Security numbers, the [AGENCY] shall request each SSN in a manner that makes the SSN easily redacted if required to be released as part of a public records request. "Redact" means to alter or truncate data so that no more than five sequential digits of a Social Security number are accessible as part of personal information.

Employee Access to Social Security Numbers

Only employees who are required to use or handle information or documents that contain SSNs will have access. All employees who have access to SSNs are trained to protect the confidentiality of SSNs.

responsibilities; and, if disclosing to a contractor or subcontractor, prior to such disclosure, the governmental entity must first receive from the contractor or subcontractor a copy of the contractor's or subcontractor's policy that sets forth how the requirements imposed under this Act on a governmental entity to protect an individual's Social Security number will be achieved.

(2) The disclosure of Social Security numbers pursuant to a court order, warrant, or subpoena.

(3) The collection, use, or disclosure of Social Security numbers in order to ensure the safety of: State and local government employees; persons committed to correctional facilities, local jails, and other law-enforcement facilities or retention centers; wards of the State; and all persons working in or visiting a State or local government agency facility.

(4) The collection, use, or disclosure of Social Security numbers for internal verification or administrative purposes.

(5) The disclosure of Social Security numbers by a State agency to any entity for the collection of delinquent child support or of any State debt or to a governmental agency to assist with an investigation or the prevention of fraud.

(6) The collection or use of Social Security numbers to investigate or prevent fraud, to conduct background checks, to collect a debt, to obtain a credit report from a consumer reporting agency under the federal Fair Credit Reporting Act, to undertake any permissible purpose that is enumerated under the federal Gramm Leach Bliley Act, or to locate a missing person, a lost relative, or a person who is due a benefit, such as a pension benefit or an unclaimed property benefit.

APPENDIX B – Template Statement of Purpose(s)

What does the [AGENCY] do with your Social Security Number?

Statement of Purpose for Collection of Social Security Numbers Identity-Protection Policy

The Identity Protection Act, 5 ILCS 179/1 *et seq.*, requires each local and State government agency to draft, approve, and implement an Identity-Protection Policy that includes a statement of the purpose or purposes for which the agency is collecting and using an individual's Social Security number (SSN). This statement of purpose is being provided to you because you have been asked by the [AGENCY] to provide your SSN or because you requested a copy of this statement.

Why do we collect your Social Security number?

You are being asked for your SSN for one or more of the following reasons:

[THE FOLLOWING PURPOSES MAY NOT APPLY; IDENTIFY PURPOSES
APPROPRIATE FOR YOUR AGENCY]

- Complaint mediation or investigation;
- Crime victim compensation;
- Vendor services, such as executing contracts and/or billing;
- Law enforcement investigation;
- Child support collection;
- Internal verification;
- Administrative services; and/or
- Other: _____

What do we do with your Social Security number?

- We will only use your SSN for the purpose for which it was collected.
- We will not:
 - Sell, lease, loan, trade, or rent your SSN to a third party for any purpose;
 - Publicly post or publicly display your SSN;
 - Print your SSN on any card required for you to access our services;
 - Require you to transmit your SSN over the Internet, unless the connection is secure or your SSN is encrypted; or
 - Print your SSN on any materials that are mailed to you, unless State or Federal law requires that number to be on documents mailed to you, or unless we are confirming the accuracy of your SSN.

Questions or Complaints about this Statement of Purpose

Write to the [AGENCY]:

[CONTACT INFORMATION]

APPENDIX C & D – Raoul Leads 50 AGs in Largest Data Breach Settlement in History...

http://www.illinoisattorneygeneral.gov/pressroom/2019_07/20190722.html

July 22, 2019

**ATTORNEY GENERAL RAOUL ANNOUNCES \$600 MILLION
SETTLEMENT WITH EQUIFAX**
***Raoul Leads 50 AGs in Largest Data Breach Settlement in History
That Includes up to \$425 Million in Consumer Restitution***

Chicago — Attorney General Kwame Raoul today announced a \$600 million settlement with Equifax that resolves a nationwide investigation into consumer reporting agency Equifax. Raoul's office led a coalition of 50 attorneys general investigating Equifax's 2017 data breach, and today's settlement represents the largest data breach settlement in history. Raoul's office opened the multistate investigation in September 2017 following the massive data breach. The investigation found that Equifax's failure to maintain a reasonable security system enabled hackers to penetrate its systems, exposing the data of 56 percent of American adults and making it the largest-ever breach of consumer data. Raoul's settlement with Equifax includes a Consumer Restitution Fund of up to \$425 million, a \$175 million payment to the states that includes more than \$7.3 million for Illinois, and injunctive relief that also includes a significant financial commitment.

"The Equifax data breach compromised the personal information of millions of Illinoisans," Raoul said. "This historic settlement should send the message that companies – particularly those tasked with protecting personal information – will be held accountable for not doing enough to keep consumers' sensitive, personal information secured."

On Sept. 7, 2017, Equifax, one of the largest consumer reporting agencies in the world, announced a data breach affecting more than 147 million consumers – nearly half of the U.S. population. In Illinois alone, an estimated 5.4 million residents were impacted. Compromised information included names, social security numbers, dates of birth, addresses, credit card numbers, and in some cases, driver's license numbers.

Shortly after, Raoul led a coalition that grew to 50 attorneys general in a multistate investigation into the breach. The investigation found that the breach occurred because Equifax failed to implement an adequate security program to protect consumers' highly sensitive personal information. Despite knowing about a critical vulnerability in its software, Equifax failed to patch its systems fully. Moreover, Equifax failed to replace software that monitored

the breached network for suspicious activity. As a result, attackers penetrated Equifax's system and went unnoticed for 76 days.

Under the terms of the settlement, Equifax agreed to provide a single Consumer Restitution Fund of up to \$425 million dedicated to consumer restitution. If the initial \$300 million is exhausted, Equifax will pay up to an additional \$125 million into the fund to cover remaining claims. The restitution program will be conducted in connection with settlements that have been reached in separate multi-district class action lawsuits filed against Equifax, as well as settlements that were reached with the Federal Trade Commission and Consumer Financial Protection Bureau. The settlement also requires Equifax to offer affected consumers extended credit monitoring services for 10 years.

A website has been established to accept claim forms and administer the settlement fund. That website, www.EquifaxBreachSettlement.com, will go live in the coming days as the settlement must be approved by the judge before the administrator can accept consumer claim forms. If consumers wish to be notified when the breach settlement website begins accepting claims against the settlement fund, they can go to <https://www.ftc.gov/equifax-data-breach> and submit their email addresses. This site, run by the Federal Trade Commission, will notify consumers who submit their email address when claims begin being accepted. For questions about eligibility for restitution, filing a claim, enrolling in credit monitoring, or additional information, people should visit www.EquifaxBreachSettlement.com or they can also call 1-833-759-2982. Individuals will be able to submit claims on the website or by mail.

Under the settlement, Equifax has also agreed to take the following steps to assist people who are facing identity theft issues or who have already had their identities stolen:

- Making it easier for consumers to freeze and thaw their credit.
- Making it easier for consumers to dispute inaccurate information in credit reports.
- Maintaining sufficient staff dedicated to assisting consumers who may be victims of identity theft.

Equifax has also agreed to incorporate to strengthen its security practices going forward, including, by:

- Reorganizing its data security team.
- Minimizing its collection of sensitive data and the use of people's social security numbers.
- Performing regular security monitoring, logging and testing.
- Employing improved access control and account management tools.

- Reorganizing and segmenting its network.
- Reorganizing its patch management team, and implementing new policies to identify and implement critical security updates and patches.

In addition to Raoul, other attorneys general participating in this settlement include Alabama, Alaska, Arizona, Arkansas, California, Colorado, Connecticut, Delaware, the District of Columbia, Florida, Georgia, Hawaii, Idaho, Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland, Michigan, Minnesota, Mississippi, Missouri, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New Mexico, New York, North Carolina, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, Puerto Rico, Rhode Island, South Carolina, South Dakota, Tennessee, Texas, Utah, Vermont, Virginia, Washington, West Virginia, Wisconsin, and Wyoming.

Privacy Unit Chief Matt Van Hise, Consumer Fraud Bureau Chief Beth Blackston, and Assistant Attorney General Ronak Shah handled the historic settlement for Raoul's Consumer Fraud Bureau.