OFFICE OF THE ATTORNEY GENERAL
STATE OF ILLINOIS

Kwame Raoul
ATTORNEY GENERAL

December 28, 2020

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

Dear Designated Task Force Recipient,

In accordance with 20 ILCS 4040/10, attached for your review and records is a copy of the Social Security Number Protection Task Force Report for 2020.

Thank you.

Best Regards,

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: 2020 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 28, 2020

CONTENTS

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 – ***Awaiting Additional Member Appointment Confirmation*****, 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 Felix Canizares**
- 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 – **Jessica Klaus**
- One member representing Central Management Services – **Jake Altman**
- 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 – **Katelyn Nassin**
- 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: Privacy Unit Chief 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)

BATTLING SYNTHETIC IDENTITY THEFT

As with the daily evolution of technology, the evolution of fraud and identity theft continues to become more sophisticated and advanced. Since the Illinois Attorney General's Office's creation of the nation's first dedicated Identity Theft Unit, the Attorney General's Office has received and assisted with over forty-eight thousand one-hundred complaints involving the identity theft of Illinois consumers. The types of identity theft typically seen include, but are not limited to: financial identity theft, medical identity theft, criminal identity theft, child identity theft, medical identity theft, tax identity theft, employment identity theft, government benefit identity theft, and one of the most pernicious and difficult to resolve, synthetic identity theft.

Synthetic identity theft occurs when a fraudster combines real and fake information to create a new identity. Once the new identity is established, the fraudster perpetuates the harm by opening new unauthorized accounts, credit lines, and by making other purchases, all with the intent of receiving the unlawful benefit while leaving the victims to link together the trail of what's happened.

Tracking and identifying synthetic identity theft is often very difficult due to the mixed reporting of accurate and false information to the major credit reporting agencies. Synthetic identity theft also often results in a higher than usual dismissal rate since new credit lines are frequently dismissed as accounting errors or outliers primarily as a result of the numerous individuals' information being utilized in creating the fraudulent identity. Ultimately, this all translates to longer than average detection times, which in turn creates more difficulty in tracking the start point of the fraud. McKinsey, an American consulting firm, reviewed 15,000 profiles from a consumer-marketing database to evaluate accuracy and likelihood of fraudulent activity and their results estimate that synthetic fraud is the fastest-growing type of financial crimes in the United States. [1] The Federal Reserve drafted a white paper specifically to address this issue in July 2019.[2]

To help combat synthetic identity theft, on May 24, 2018, Congress enacted the Economic Growth, Regulatory Relief, and Consumer Protection Act.[3] Section 215 of this act requires the U.S. Social Security Administration ("SSA") to build a system for financial institutions capable of real time verification of whether a name, date of birth, and Social Security number are a match with what the SSA currently has in their database, often referred to as the electronic Consent Based Social Security Verification ("eCBSV") service. Through the use of this database, financial institutions and service providers will be able to validate identities much more quickly. Financial entities must apply to SSA to gain access to the database, and once permitted, will be able to validate their information on file with the information from SSA more expediently. This law targets synthetic identity theft by streamlining the process for financial institutions to verify that the personal information on file with the financial institution is consistent with the personal information on file with the SSA, and does not demonstrate a patchwork of real and fake information. The goal of the eCBSV would be to provide a useful tool to financial institutions to prevent identity theft at the application stage, before financial harm is passed on to the consumer.

Initial rollout for eCBSV was mid 2020 and was limited to support the testing, development, and capacity of the product, but new applications were opened on November 30, 2020. Congress passed the Taxpayer First Act in July 2019 directing the Internal Revenue Service to build a similar verification system that would allow lenders to validate certain tax data provided by applicants.[4]

While it is still early in the rollout for eCBSV, there is hope that cooperation between the private and public sector will help produce mutually beneficial outcomes and increase the potential for further technological and legislative developments to improve our ability to catch bad actors before financial harm is passed to the consumers.

The eCBSV and the Taxpayer First Act are strong examples of the importance of public-private collaboration in order to challenge the increasing sophistication of bad actors. State and Federal

---

[1] https://www.mckinsey.com/business-functions/risk/our-insights/fighting-back-against-synthetic-identity-fraud
[2] https://fedpaymentsimprovement.org/wp-content/uploads/frs-synthetic-identity-payments-fraud-white-paper-july-2019.pdf
[3] Public Law No: 115-174
[4] Public Law No: 116-25

agencies should continue to develop new tools and strategies to combat identity fraud and theft, and secure Social Security numbers.

(Section 215 of Public Law No: 115-174 – 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. On September 30, 2020, Illinois was part of a $39.5 million dollar settlement with 43 states with the health insurance company Anthem. The Attorney General's settlement stemmed from Anthem's 2014 data breach that involved 78.8 million American's personal information, including 1.7 million Illinois residents. Included within the compromised information was data harvested from Anthem's data warehouse, which contained highly sensitive personal information, including SSNs.

As part of that settlement, Anthem agreed to ensure compliance with zero trust architecture principles, which are designed to limit access to sensitive data, and minimize access to sensitive personal information such as SSNs. The settlement also requires Anthem to regularly monitor and inspect network traffic, authorize device and network activity within the network, and require appropriate authorization prior to any user's access to the network. These requirements, among many others, aim at the goal of limiting access of SSNs to permitted users only, as well as to carefully log what devices have access in order to monitor and detect fraudulent activity.

The September 2020 settlement also requires Anthem to implement and maintain appropriate access controls of all accounts with access to personal information or protected health information, including individual accounts, administrator accounts, service accounts, and vendor accounts. These controls include a means to regularly review and assess the access levels of users, as well as to ensure the expeditious removal of access for employees after severing employment.

(*Attorney General Raoul Announces $39.5 Million Settlement with Anthem Over 2014 Data Breach* – Appendix D)

TASK FORCE APPOINTMENTS & UPDATES

The Task Force awaits calendar year 2021 Appointment and Confirmations for the following currently vacant membership seats:

- (1) Member representing the House of Representatives, Appointed by the Speaker of the House;
- (1) Member representing the Senate, Appointed by the President of the Senate;
- (2) Members representing the Senate, Appointed by the Minority Leader of the Senate; and
- (1) Member representing the Office of the Governor;

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 not[5]:

---

[5] 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— Section 215 of Public Law No: 115-174

SEC. 215. <<NOTE: 42 USC 405b.>> REDUCING IDENTITY FRAUD.

(a) Purpose.--The purpose of this section is to reduce the prevalence of synthetic identity fraud, which disproportionally affects vulnerable populations, such as minors and recent immigrants, by facilitating the validation by permitted entities of fraud protection data, pursuant to electronically received consumer consent, through use of a database maintained by the Commissioner.

(b) Definitions.--In this section:

(1) Commissioner.--The term ``Commissioner'' means the Commissioner of the Social Security Administration.

(2) Financial institution.--The term ``financial institution'' has the meaning given the term in section 509 of the Gramm-Leach-Bliley Act (15 U.S.C. 6809).

(3) Fraud protection data.--The term ``fraud protection data'' means a combination of the following information with respect to an individual:

(A) The name of the individual (including the first name and any family forename or surname of the individual).

(B) The social security number of the individual.

(C) The date of birth (including the month, day, and year) of the individual.

(4) Permitted entity.--The term ``permitted entity'' means a financial institution or a service provider, subsidiary, affiliate, agent, subcontractor, or assignee of a financial institution.

(c) Efficiency.--

(1) Reliance on existing methods.--The Commissioner shall evaluate the feasibility of making modifications to any database that is in existence as of the date of enactment of this Act or a similar resource such that the database or resource--

(A) is reasonably designed to effectuate the purpose of this section; and

(B) meets the requirements of subsection (d).

(2) Execution.--The Commissioner shall make the modifications necessary to any database that is in existence as of the date of enactment of this Act or similar resource, or develop a database or similar resource, to effectuate the requirements described in paragraph (1).

(d) Protection of Vulnerable Consumers.--The database or similar resource described in subsection (c) shall--

(1) compare fraud protection data provided in an inquiry by a permitted entity against such information maintained by the Commissioner in order to confirm (or not confirm) the validity of the information provided;

(2) be scalable and accommodate reasonably anticipated volumes of verification requests from permitted entities with commercially reasonable uptime and availability; and

(3) allow permitted entities to submit--

(A) 1 or more individual requests electronically for real-time machine-to-machine (or similar functionality) accurate responses; and

(B) multiple requests electronically, such as those provided in a batch format, for accurate electronic responses within a reasonable period of time from submission, not to exceed 24 hours.

(e) <<NOTE: Deadline.>> Certification Required.--Before providing confirmation of fraud protection data to a permitted entity, the Commissioner shall ensure that the Commissioner has a certification from the permitted entity that is dated not more than 2 years before the date on which that confirmation is provided that includes the following declarations:

(1) The entity is a permitted entity.

(2) The entity is in compliance with this section.

(3) The entity is, and will remain, in compliance with its privacy and data security requirements, as described in title V of the Gramm-Leach-Bliley Act (15 U.S.C. 6801 et seq.), with respect to information the entity receives from the Commissioner pursuant to this section.

(4) <<NOTE: Time period.>> The entity will retain sufficient records to demonstrate its compliance with its certification and this section for a period of not less than 2 years.

(f) Consumer Consent.--

(1) In general.--Notwithstanding any other provision of law or regulation, a permitted entity may submit a request to the database or similar resource described in subsection (c) only--

(A) pursuant to the written, including electronic, consent received by a permitted entity from the individual who is the subject of the request; and

(B) in connection with a credit transaction or any circumstance described in section 604 of the Fair Credit Reporting Act (15 U.S.C. 1681b).

(2) Electronic consent requirements.--For a permitted entity

to use the consent of an individual received electronically pursuant to paragraph (1)(A), the permitted entity must obtain the individual's electronic signature, as defined in section 106 of the Electronic Signatures in Global and National Commerce Act (15 U.S.C. 7006).

(3) Effectuating electronic consent.--No provision of law or requirement, including section 552a of title 5, United States Code, shall prevent the use of electronic consent for purposes of this subsection or for use in any other consent based verification under the discretion of the Commissioner.

(g) Compliance and Enforcement.--

(1) Audits and monitoring.--The Commissioner may--

(A) conduct audits and monitoring to--

(i) ensure proper use by permitted entities of the database or similar resource described in subsection (c); and

(ii) deter fraud and misuse by permitted entities with respect to the database or similar resource described in subsection (c); and

(B) terminate services for any permitted entity that prevents or refuses to allow the Commissioner to carry out the activities described in subparagraph (A).

(2) Enforcement.--

(A) In general.--Notwithstanding any other provision of law, including the matter preceding paragraph (1) of section 505(a) of the Gramm-Leach-Bliley Act (15 U.S.C. 6805(a)), any violation of this section and any certification made under this section shall be enforced in accordance with paragraphs (1) through (7) of such section 505(a) by the agencies described in those paragraphs.

(B) Relevant information.--Upon discovery by the Commissioner, pursuant to an audit described in paragraph (1), of any violation of this section or any certification made under this section, the Commissioner shall forward any relevant information pertaining to that violation to the appropriate agency described in subparagraph (A) for evaluation by the agency for purposes of enforcing this section.

(h) Recovery of Costs.--

(1) In general.--

(A) In general.--Amounts obligated to carry out this section shall be fully recovered from the users of the database or verification system by way of advances, reimbursements, user fees, or other recoveries as

determined by the Commissioner. The funds recovered under this paragraph shall be deposited as an offsetting collection to the account providing appropriations for the Social Security Administration, to be used for the administration of this section without fiscal year limitation.

(B) Prices fixed by commissioner.--The Commissioner shall establish the amount to be paid by the users under this paragraph, including the costs of any services or work performed, such as any appropriate upgrades, maintenance, and associated direct and indirect administrative costs, in support of carrying out the purposes described in this section, by reimbursement or in advance as determined by the Commissioner. The amount of such prices shall be periodically adjusted by the Commissioner to ensure that amounts collected are sufficient to fully offset the cost of the administration of this section.

(2) Initial development.--The Commissioner shall not begin development of a verification system to carry out this section until the Commissioner determines that amounts equal to at least 50 percent of program start-up costs have been collected under paragraph (1).

(3) Existing resources.--The Commissioner may use funds designated for information technology modernization to carry out this section.

(4) Annual report.--The Commissioner shall annually submit to the Committee on Ways and Means of the House of Representatives and the Committee on Finance of the Senate a report on the amount of indirect costs to the Social Security Administration arising as a result of the implementation of this section.

APPENDIX D – Attorney General Raoul Announces $39.5 Million Settlement with Anthem…

https://illinoisattorneygeneral.gov/pressroom/2020_09/20200930.html

ATTORNEY GENERAL RAOUL ANNOUNCES $39.5 MILLION SETTLEMENT WITH ANTHEM OVER 2014 DATA BREACH

Settlement Includes More Than $1.7 Million for Illinois and Requires Anthem to Improve Security Measures

Chicago — Attorney General Kwame Raoul today joined a coalition of 43 attorneys general in announcing a $39.5 million settlement with the health insurance company Anthem Inc. stemming from the massive 2014 data breach that involved the personal information of more than 78 million Americans. Raoul's office was part of the executive committee negotiating the settlement, Illinois and will receive more than $1.7 million. In addition to the payment, Anthem Inc. (Anthem) has also agreed to a series of data security and good governance provisions designed to strengthen its security practices moving forward.

In February 2015, Anthem disclosed that, beginning in February 2014, cyber attackers had infiltrated its systems using malware installed through a phishing email. The attackers were ultimately able to gain access to Anthem's data warehouse, where they harvested names, dates of birth, Social Security numbers, health care identification numbers, home addresses, email addresses, phone numbers, and employment information for 78.8 million Americans, including more than 1.7 million Illinois residents.

"The Anthem data breach compromised the personal information of more than 1 million Illinois residents," Raoul said. "Today's settlement ensures that Anthem prioritizes protecting consumer data with protections designed to prevent future data breaches This settlement sends the message that companies will be held accountable for not doing enough to keep consumers' personal information secured."

Under the settlement, Anthem has also agreed to a series of provisions designed to strengthen its security practices, including:

- Prohibiting misrepresentations regarding the extent to which Anthem protects the privacy and security of personal information.
- Implementing a comprehensive information security program, incorporating principles of zero trust architecture, and including regular security reporting to the board of directors and prompt notice of significant security events to the CEO.
- Implementing specific security requirements with respect to segmentation, logging and monitoring, anti-virus maintenance, access controls and two factor authentication, encryption, risk assessments, penetration testing, and employee training, among other requirements.
- Implementing third-party security assessments and audits for three years, as well as requiring that Anthem make its risk assessments available to a third-party assessor during that term.

The scam started by "phishing" for a consumer's personal and financial information by sending phony but official-looking emails that included links designed for the consumer to click on, which triggered malware to be installed on a consumer's computer to steal their information. Phishing scams also originated over the phone when a caller claiming to represent Anthem sought to extract personal or financial information from a consumer.

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

Joining Raoul in the settlement are the attorneys general of Alaska, Arizona, Arkansas, Colorado, Connecticut, the District of Columbia, Delaware, Florida, Georgia, Hawaii, Idaho, Indiana, Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland, Michigan, Minnesota, Mississippi, Missouri, Nebraska, New Hampshire, New Jersey, New York, Nevada, North Carolina, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Carolina, Tennessee, Texas, Virginia, Washington, West Virginia and Wisconsin.