

Social Security Number Protection Task Force
Report to the Illinois General Assembly, Governor Pat Quinn,
and Secretary of State Jesse White
December 31, 2010

CONTENTS

- I. Task Force Background
 - a. Membership of the Task Force
- II. Part I: Protection of SSNs in the Public Record
 - a. Identity Protection Act
 - b. Federal Red Flag Guidelines
- III. Part II: SSNs as Internal Identifiers
 - a. State and Local Agency Implementation of Unique Identifiers
- IV. Task Force Appointments
- V. Conclusion

APPENDIX A – TEMPLATE IDENTITY PROTECTION POLICY

APPENDIX B – TEMPLATE STATEMENT OF PURPOSE(S)

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 in these records 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 the 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 John Fritchey, Representative Sara Feigenholtz**
- Two members representing the House of Representatives, appointed by the Minority Leader of the House – **Representative Sandra Pihos, TBA**
- Two members representing the Senate, appointed by the President of the Senate – **Senator Jeffrey Schoenberg, Senator Jacqueline Collins**
- Two members representing the Senate, appointed by the Minority Leader of the Senate – **Senator Chris Lauzen, Senator Dan Duffy**
- One member representing the Office of the Attorney General – **Deborah Hagan, Task Force Chair**
- One member representing the Office of the Secretary of State – **Micah Miller**
- One member representing the Office of the Governor – **Jay Stewart**
- One member representing the Department of Natural Resources – **J.J. Pohlman**
- One member representing the Department of Healthcare and Family Services – **Tamara Hoffman**
- One member representing the Department of Revenue – **George Logan**

- One member representing the Department of State Police – **Patrick Keen**
- 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 – **Patricia Carter**
- One member representing Central Management Services – **Robert Morgan**
- One member appointed by the Executive Director of the Board of Higher Education – **Don Sevenser**
- One member appointed by the Secretary of Human Services – **Solomon Oriakhi**
- Three members representing local-governmental organizations – **Dorothy Brown, Larry Reinhardt, Virginia Hayden**
- One member representing the Office of the State Comptroller – **Whitney Rosen**
- 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 Social Security number (SSN).

Identity Protection Act

On May 28, 2009, both houses passed HB547, which creates the Identity Protection Act. It was sent to the Governor on June 26, 2009 and the Governor issued an Amendatory Veto on August 25, 2009. The House accepted the Governor's Amendatory Veto on October 14, 2009 and the Senate accepted the Governor's Amendatory Veto on October 30, 2009. On January 22, 2010, the Governor certified the changes and signed the bill. The effective date of the Act was June 1, 2010.

The Identity Protection Act (5 ILCS 179/1 *et seq.*) prohibits a person, or State or local government agency from publicly posting or displaying the SSN; printing the SSN on cards required for access to products or services; requiring an individual to transmit his or her SSN over the Internet, unless the connection is secure or the SSN is encrypted; or printing an SSN on any materials that are mailed, with exceptions. These prohibitions went into effect July 1, 2010.

Also beginning July 1, 2010, no person or State or local government agency may collect, use, or disclose a SSN unless required to do so under state or federal law; the need and purpose for the SSN is documented before the request; and the SSN collected is relevant to the documented need and purpose. There are several exceptions to the prohibitions in this section.

A person or State or local government agency must 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 SSN. A person or State or local government agency must redact SSNs from the information or documents before allowing the public inspection or copying of the information or documents.

The Act does not apply to collection, use, or release of a SSN as required by State or federal law, rule, or regulation, or the use of SSN or other identifying information for internal verification or

administrative purposes. The Act does not apply to documents that are recorded with a county recorder or required to be open to the public under any State or federal law, rule, or regulation, applicable case law, Supreme Court Rule, or the Constitution of the State of Illinois.

Local and State governmental agencies, including county recorders, are required to draft and approve an Identity-Protection Policy.

- The Effective Date of this provision of the Act is **June 1, 2010**.
- An entity's Identity-Protection Policy, which includes a statement of the purpose(s) for the collection of Social Security numbers, must be **approved no later than June 1, 2011**.
- An entity's Identity-Protection Policy must be **implemented within 12 months of the date of approval** (no later than June 1, 2012).

The Identity Protection Policy must:

- require all employees who have access to SSNs to be trained to protect the confidentiality of SSNs;
- direct that only employees who are required to use or handle information or documents that contain SSNs to have access;
- require that SSNs requested from individuals be provided in a manner that makes the SSN easily redacted; and
- require that, when collecting SSNs, a statement of the purpose or purposes for which the agency is collecting and using the SSN be provided.

On June 4, 2010, the Office of the Attorney General provided a Template Identity-Protection Policy and Statement of Purpose to the SSN Protection Task Force members. These documents are attached as Exhibit A and Exhibit B. In addition, that Template has since been provided to local and State governmental agencies upon request.

The Judicial branch and clerks of court are not subject to provisions of the Act, but the Supreme Court is required under its rulemaking authority to adopt requirements applicable to the judicial branch, including clerks of court, regulating the disclosure of SSNs.

Federal Red Flag Guidelines

The FTC is set to begin enforcing the Federal Red Flag Guidelines, which require all financial institutions and creditors to develop and implement a written Identity Theft Prevention Program that is designed to detect, prevent, and mitigate identity theft, on December 31, 2010.

Enforcement by the FTC had been delayed several times. The delays were necessary in part to allow Congress to clarify the scope of the Red Flag Guidelines. The definition of a "creditor" was originally very broad, and included many entities that had not historically been considered creditors.

On December 1, 2010, Congress passed Senate bill 3987, the "Red Flag Program Clarification Act of 2010." The Act amends the Fair Credit Reporting Act by clarifying the definition of a creditor. Under the Act, the term creditor does not include a creditor that advances funds on behalf of a person for expenses incidental to a service provided by the creditor to that person. Senator Christopher Dodd (D-Connecticut), in a Colloquy in Support of Legislation Clarifying

the Definition of Creditor under the FTC “Red Flags” Rule, said that the bill “makes clear that lawyers, doctors, dentists, orthodontists, pharmacists, veterinarians, accountants, nurse practitioners, social workers, other types of health care providers and other service providers will no longer be classified as ‘creditors’ for the purposes of the Red Flags Rule just because they do not receive payment in full from their clients at the time they provide their services, when they don’t offer or maintain accounts that pose a reasonably foreseeable risk of identity theft.” Senate bill 3987 became Public Law 111-319 on December 18, 2010.

Even with the clarification to the definition of a “creditor,” a state or local government agency may still be required to fulfill the obligations of the Red Flag Guidelines. Each agency is encouraged to assess its own business practices and determine if the advancing of funds is incidental to the service provided.

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 Agency Implementation of Unique Identifiers

State and local government agencies continue to internally assess the collection and use of SSNs. Such an assessment will be critical as agencies draft and implement their Identity Protection Policies pursuant to Public Law 96-874.

Department of Human Services

The Department of Human Services continues to implement a unique identification number system for clients. Through collaborative efforts, DHS has assigned over one million Recipient Identification Numbers (RINs) for customers who receive DHS services provided by Mental Health, Developmental Disabilities, Rehabilitation Services, Community Health and Prevention, and Alcoholism and Substance Abuse. Previously, RINs had only been used by the Division of Human Capital Development (HCD), the DHS department that provides customers with cash, medical, and food stamp benefits. Regardless of the services received, a customer should have a single RIN. Those customers who have received a RIN for cash, medical, or food stamp benefits will be reassessed by DHS to determine if that RIN can be used for other services. Coordinating across DHS departments is integral to the success of the RIN system.

The seven Illinois agencies charged with delivering healthcare and human services to state residents have begun to work together to improve the delivery of these services to residents in need. This collaborative effort, called the Framework, brings together Department on Aging, Department of Children & Family Services, Department of Commerce and Economic Opportunity, Department of Employment Security, Department of Healthcare & Family Services, Department of Human Services, and Department of Public Health. These agencies that are a part of the Framework have already identified areas of focus including improving customer service and modernizing technology. Currently, customers of these agencies do not receive a single, unique

identification number. Such a number may assist the Framework in meeting its goal of streamlining data sharing between agencies without compromising the security of sensitive personally identifiable information. The Framework has initiated an effort to establish a single client identifier across these seven agencies and in doing so will build upon the work that DHS has already begun on the RIN.

TASK FORCE APPOINTMENTS

Many members of the Task Force were appointed soon after the Task Force became effective, and in 2007 and 2008 when more appointments became necessary. The following recent appointments have been made to the Task Force.

On March 8, 2010, Robert Morgan was appointed to the Task Force to represent Central Management Services.

On April 29, 2010, Senator Dan Duffy was appointed to the Task Force by the Senate Minority Leader.

CONCLUSION

With the passage and signing of the Identity Protection Act, Illinois has taken a necessary step in protecting against the widespread dissemination of Social Security numbers. The new law requires state and local government agencies to take a more active role in the fight against identity theft. The Task Force membership 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,

- 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.

contractors, or subcontractors if disclosure is necessary in order for the entity to perform its duties and 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]