Social Security Number Protection Task Force Report 2011
Report to the Illinois General Assembly, Governor Pat Quinn,
and Secretary of State Jesse White
December 31, 2011

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.

To determine the best methods for protecting SSNs and limiting their widespread dissemination and potential misuse, many jurisdictions turn to the Fair Information Practice Principles (FIPPs), a universally accepted framework for privacy protections. The FIPPs have been used in this country since the mid-1970s, when they formed the basis for many of the concepts in the federal Privacy Act of 1974. Internationally, the Organisation for Economic Co-operation and Development's ("OECD") privacy guidelines include the following principles: collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability. At their core, the FIPPs consist of: (1) Notice/Awareness; (2) Choice/Consent; (3) Access/Participation; (4) Integrity/Security; and (5) Enforcement/Redress.

Many of these same concepts have now also been integrated into Illinois law. 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 enacting Public Act 95-0482. The Office of the Attorney General is charged with chairing and administering the activities of the Task Force.

The Task Force brings together representatives from many state agencies and constitutional offices to address these timely issues, and ultimately to recommend rules, regulations or legislation that will prevent the further dissemination of SSNs.

Membership of the Task Force:

- Two members representing the House of Representatives, appointed by the Speaker of the House – **Representative Sara Feigenholtz,** vacant
- Two members representing the House of Representatives, appointed by the Minority Leader of the House – **Representative Sandra Pihos, Representative Kay Hatcher**
- 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 – vacant
- One member representing the Department of Healthcare and Family Services – vacant
- 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 – vacant
- One member representing Central Management Services – **Robert Morgan**
- One member appointed by the Executive Director of the Board of Higher Education – vacant
- One member appointed by the Secretary of Human Services – vacant
- Three members representing local-governmental organizations – **Dorothy Brown, Larry Reinhardt, Virginia Hayden**
- One member representing the Office of the State Comptroller – vacant
- 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 government 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
SSN Protection Task Force
100 W. Randolph, 12th Floor
Chicago, IL 60601

At entity's Identity-Protection Policy must be **implemented within 12 months of the date of approval** (no later than June 1, 2012). 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 collection through the destruction of the information.

Illinois Supreme Court Rule 138

The Illinois Supreme Court has adopted Rule 138 pursuant to Section 40 of the Identity Protection Act. Section 40 of the Identity Protection Act, 5 ILCS 179, requires the Supreme Court, under its rulemaking authority or by administrative order, to adopt requirements applicable to the judicial branch, including clerks of the circuit court, regulating the disclosure of social security numbers consistent with the intent of the Act and the unique circumstances relevant in the judicial process. The effective date of Rule 138 is January 1, 2012.

> Rule 138. Social Security Numbers in Pleadings and Related Matters.
> (a) Unless otherwise required by law or ordered by the court, parties shall not include Social Security numbers in documents filed with the court, including exhibits thereto, whether filed electronically or in paper. If disclosure of an individual's Social Security number is required for a particular filing, only the last four digits of that number shall be used. The filing must be accompanied by a confidential information form in substantial compliance with the attached NOTICE OF CONFIDENTIAL INFORMATION WITHIN COURT FILING, which shall identify the full Social Security number and shall remain confidential, except as to the parties or as the court may direct. *[See Notice of Confidential Information within Court Filing Sample Form, attached hereto as Appendix A.]*
>
> (b) Neither the court, nor the clerk, will review each pleading for compliance with this rule. If a pleading is filed without redaction, a party or identified person may move the court to order redaction. If the court finds the inclusion of the Social Security number was willful, the court may award the prevailing party reasonable

expenses, including attorney fees and court costs, incurred in making or opposing the motion.

(c) This rule does not require any party, attorney, clerk or judicial officer to redact information from a court record that was filed prior to the adoption of this rule; provided, however, that a party may request that a Social Security number be redacted in a matter that preceded the adoption of this rule.

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. Ongoing assessments will be necessary as those policies are implemented in the coming months.

PERSONAL INFORMATION PROTECTION ACT

Public Act 97-0483, enacted August 22, 2011, amends the Personal Information Protection Act (PIPA). The changes to PIPA are effective January 1, 2012.

PIPA requires entities that suffer security breaches of personal information to notify affected individuals without unreasonable delay. Notification in the event of a breach allows affected individuals to take steps to protect themselves against identity theft or other financial fraud. A breach is defined as the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information, where personal information is an individual's name combined with SSN, driver's license number, or financial account number. It is important for Task Force members to be aware of the requirements of PIPA because the Act applies to state agencies that collect this data. In addition, although the breach notification is limited to computerized data for most entities, notification must go out from state agencies when there has been a breach of *written* material as well as computerized data.

The first change made by Public Act 97-0483 requires entities to include specific information in the breach notification letter. The disclosure notification to an Illinois resident shall include, but need not be limited to:

(i) the toll-free numbers and addresses for consumer reporting agencies,
(ii) the toll-free number, address, and website address for the Federal Trade Commission, and
(iii) a statement that the individual can obtain information from these sources about fraud alerts and security freezes.

The notification shall not, however, include information concerning the number of Illinois residents affected by the breach.

The amendment also clarifies the responsibilities of data collectors that maintain personal information, but do not own or license such information. Under existing law, entities that maintain the data that suffer breaches must notify the data owner immediately upon discovery of the breach. The amendment adds the following requirement:

> In addition to providing such notification to the owner or licensee, the data collector shall cooperate with the owner or licensee in matters relating to the breach. That cooperation shall include, but need not be limited to, (i) informing the owner or licensee of the breach, including giving notice of the date or approximate date of the breach and the nature of the breach, and (ii) informing the owner or licensee of any steps the data collector has taken or plans to take relating to the breach. The data collector's cooperation shall not, however, be deemed to require either the disclosure of confidential business information or trade secrets or the notification of an Illinois resident who may have been affected by the breach.

Lastly, PIPA is amended by adding a new section for the proper disposal of materials containing personal information. Proper disposal of material that contains personal information is a necessary step in protecting individuals against identity theft and financial fraud. Incidents of identity theft occur when "dumpster divers" find troves of valuable personal information in publicly available garbage bins. In addition, personal information left on computers and other electronic media can be accessed and misused with relative ease.

There are several federal requirements for proper disposal of materials containing personal information. The Safeguards Rule, a federal regulation that implements the Gramm-Leach-Bliley Act, obligates a financial institution to protect the security and confidentiality of customers' nonpublic personal information by implementing and maintaining a written information security program that includes procedures for proper disposal. The Disposal Rule, a federal regulation that implements the Fair Credit Reporting Act, requires entities that possess or maintain consumer reports, or records derived from a consumer report, to properly dispose of those reports by taking reasonable measures to protect against unauthorized access. No such similar law existed in Illinois until now, with the addition of Section 40 to PIPA.

> Disposal of materials containing personal information; Attorney General.
>
> (a) In this Section, "person" means: a natural person; a corporation, partnership, association, or other legal entity; a unit of local government or any agency, department, division, bureau, board, commission, or committee thereof; or the State of Illinois or any constitutional officer, agency, department, division, bureau, board, commission, or committee thereof.
>
> (b) A person must dispose of the materials containing personal information in a manner that renders the personal information unreadable, unusable, and undecipherable. Proper disposal methods include, but are not limited to, the following:
>
> (1) Paper documents containing personal information may be either redacted, burned, pulverized, or shredded so that personal information cannot practicably be read or reconstructed.
>
> (2) Electronic media and other non-paper media containing personal information may be destroyed or erased so that personal information cannot practicably be read or reconstructed.
>
> (c) Any person disposing of materials containing personal information may contract with a third party to dispose of such materials in accordance with this Section. Any third party that contracts with a person to dispose of materials

containing personal information must implement and monitor compliance with policies and procedures that prohibit unauthorized access to or acquisition of or use of personal information during the collection, transportation, and disposal of materials containing personal information.

(d) Any person, including but not limited to a third party referenced in subsection (c), who violates this Section is subject to a civil penalty of not more than $100 for each individual with respect to whom personal information is disposed of in violation of this Section. A civil penalty may not, however, exceed $50,000 for each instance of improper disposal of materials containing personal information. The Attorney General may impose a civil penalty after notice to the person accused of violating this Section and an opportunity for that person to be heard in the matter. The Attorney General may file a civil action in the circuit court to recover any penalty imposed under this Section.

(e) In addition to the authority to impose a civil penalty under subsection (d), the Attorney General may bring an action in the circuit court to remedy a violation of this Section, seeking any appropriate relief.

(f) A financial institution under 15 U.S.C. 6801 *et. seq*. or any person subject to 15 U.S.C. 1681w is exempt from this Section.

TASK FORCE APPOINTMENTS

On December 12, 2011, Representative Tom Cross, House Republican Leader, appointed Representative Kay Hatcher to the Task Force.

CONCLUSION

Identity Protection Policies at local and State government agencies throughout Illinois will be implemented in the coming months. The Illinois Supreme Court and court administrators have done their part by amending the Supreme Court Rules to prohibit the filing SSNs in court documents as appropriate. These policies and changes to documents that are filed with the courts will go a long way to prevent the widespread dissemination of SSNs in the public sphere. 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

NOTICE OF CONFIDENTIAL INFORMATION WITHIN COURT FILING SAMPLE FORM

In the Circuit Court of the _____ Judicial Circuit,
_____ County, Illinois
(Or, In the Circuit Court of Cook County, Illinois)

_____	)	
Plaintiff/Petitioner,	)	
	)	Case No. _____
v.	)	
	)	
	)	
_____	)	
Defendant/Respondent,	)	

NOTICE OF CONFIDENTIAL INFORMATION WITHIN COURT FILING

Pursuant to Illinois Supreme Court Rule 138, the filer of a court record at the time of filing shall include a confidential information form which identifies the full social security numbers for any individuals whose social security numbers are redacted within the filing. This information will not be available to the public and this document will be stored in a separate location from the case file.

Party/Individual Information:

1. Name: _____
   Address: _____
   _____
   Phone: _____
   SSN: _____
2. Name: _____
   Address: _____
   _____
   Phone: _____
   SSN: _____

(Attach additional pages, if necessary.)