OFFICE OF THE ATTORNEY GENERAL
STATE OF ILLINOIS

KWAME RAOUL
ATTORNEY GENERAL

December 28, 2023

RE: Social Security Number Protection Task Force Report
to: **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 2023.

Thank you.

Best Regards,

Matthew W. Van Hise

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

Enclosure: 2023 Task Force Report

Social Security Number Protection Task Force

Report to Governor J.B. Pritzker, Attorney General Kwame Raoul,
Secretary of State Alexi Giannoulias, and Illinois General Assembly
December 28, 2023

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: Chief Privacy Officer Matthew W. Van Hise
500 S. Second Street
Springfield, IL 62701

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 SSNPolicy@ilag.gov. 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)

NEW DEVELOPMENTS IN LAWS AND REGULATIONS TO PROTECT SOCIAL SECURITY NUMBERS:

Over the last several years, this Task Force has monitored and followed the many efforts of the State of Illinois and the Federal Government as it continually updates and modifies its laws and regulations to meet the ongoing and newly emerging threats to the protection of residents' personally identifiable information. A noteworthy effort, specifically to assist with protecting SSNs, recently occurred at the federal level. The General Services Administration (GSA) issued a final ruling on May 19, 2023, to amend the Privacy Act to implement the Social Security Number Fraud Prevention Act of 2017. The GSA ruling clarified the procedural requirements for the inclusion of Social Security numbers on mailed documents sent by the GSA. In updating this language, the GSA created specified conditions that will minimize Social Security numbers included in mailed information, further protecting consumers by limiting the number of opportunities to have their physical SSNs exposed.

As highlighted above, the continued updating of laws and regulations is necessary in combatting identity theft and fraud, while at the same time, also ensuring access to individuals' personal information is available when necessary and appropriate.

(Section of the Federal Register Vol. 88, No 97 Friday, May 19, 2023, Rules and Regulations– 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

In today's world, Social Security numbers have become both an identifier and authenticator for recognizing and proving one's government-issued identity. Partly due to the proliferation of data breaches exposing consumer SSNs, minimizing the use of SSNs has become increasingly important.

A variety of laws govern the safeguarding of Illinois residents' SSNs, including the Illinois Consumer Fraud and Deceptive Business Practices Act, the Illinois Personal Information Protection Act, and the federal HIPAA Privacy and Security Rule. These law's SSN provisions provide safeguards to industries such as education, healthcare, and financial services, all which frequently require the collection of SSNs to perform essential services. With the increase of data breaches over the past decade, the duty to ensure that proper precautions are taken with SSNs is critical in minimizing the impact of an incident's effects on individual and to assist with identity theft prevention.

Even with these laws and protections in place, it's only by limiting the collection, use, and retention of SSNs that data collectors and processors can reduce the overall risk to individuals.

On October 5, 2023, Illinois announced its leadership and participation in a nationwide settlement with Blackbaud, a software company that works extensively with non-profit organizations such as K-12 schools, charities, health organizations and cultural groups, relating to a 2020 data breach that compromised the personal information of thousands of consumers nationwide, including Illinois residents. Approximately 13,000 of Blackbaud's direct customers were affected, each with clients and donors of their own whose data was stored on Blackbaud's network.

Impacted personal information associated with the breach included - consumers' names, addresses, dates of birth, Social Security numbers, contact information, financial information such as donation history, and identification numbers such as driver's license numbers, and other related information, including demographic and contact information.

As part of the settlement, Blackbaud agreed to strengthen its due diligence and data security practices going forward, specifically, by - implementing a comprehensive information security program, enacting data minimization and disposal requirements), enhancing its employee education and training process specific to its comprehensive data and information security program, and by boosting its vetting and oversight of third parties to which it provides access to consumers' personal information.

The 2023 settlement also requires Blackbaud to encrypt all databases containing Blackbaud customer data, which will help protect sensitive consumer data against potential future threats.

Included as part of the agreement, to help bolster its internal governance process, the settlement terms ensure a functioning, well-supported and resourced, Chief Information Security Officer, Chief Privacy Officer, Chief Technology Officer, and Business Information Security Officer each with clear delineated roles for implementing, maintaining, and monitoring Blackbaud's Information Security Program.

Illinois' share of the Blackbaud data breach settlement announced on October 5, 2023, was $2.28 million.

(*Attorney General Raoul Announces $49.5 Million Multistate Settlement with Blackbaud for Data Breach*– Appendix D)

TASK FORCE APPOINTMENTS & UPDATES

The Task Force awaits calendar year 2023 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[1]:

---

[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]

APPENDIX C — Section of the Federal Register Vol. 88, No 97 Friday, May 19, 2023, Rules and Regulations

PART 105–64—GSA PRIVACY ACT RULES

1. The authority citation for 41 CFR part 105–64 continues to read as follows: Authority: 5 U.S.C. 552a.

2. Amend § 105–64.001 by adding in alphabetical order the definition ‘‘Unredacted SSN Mailed Documents Listing’’ to read as follows: § 105–64.001 What terms are defined in this part?

Un-redacted SSN Mailed Documents Listing (USMDL) means the Agency approved list, as posted at www.gsa.gov/ reference/gsa-privacy-program, designating those documents for which the inclusion of the Social Security account number (SSN) is determined to be necessary to fulfill a compelling Agency business need when the documents are requested by individuals outside the Agency or other Federal agencies, as determined by the Administrator or their designee.

3. Amend § 105–64.107 by adding paragraph (c) to read as follows: § 105–64.107 What standards of conduct apply to employees with privacy-related responsibilities?

(c) (1) The following conditions must be met for the inclusion of an unredacted (full) SSN or partially redacted (truncated) SSN on any document sent by mail on behalf of the agency: (i) The inclusion of the full SSN or truncated SSN of an individual must be required or authorized by law; and (ii) The document must be listed on the USMDL. (2) Even when the conditions set forth in paragraph (c)(1) are met, employees shall redact SSNs in all documents sent by mail where feasible. Where full redaction is not possible due to agency requirements, partial redaction to create a truncated SSN shall be preferred to no redaction. (3) In no case shall any complete or partial SSN be visible on the outside of any envelope or package sent by mail or displayed on correspondence that is visible through the window of an envelope or package.

https://www.govinfo.gov/content/pkg/FR-2023-05-19/pdf/2023-10279.pdf

APPENDIX D – Attorney General Raoul Announces $49.5 Million Multistate Settlement with Blackbaud for Data Breach …

https://illinoisattorneygeneral.gov/News-Room/
October 2023.

ATTORNEY GENERAL RAOUL ANNOUNCES $49.5 MILLION MULTISTATE SETTLEMENT WITH BLACKBAUD FOR DATA BREACH

October 05, 2023

Breach Affected Thousands of Nonprofits and Millions of Consumers through U.S., Illinois to Receive $2.28 Million in Settlement

Chicago – Attorney General Kwame Raoul today announced that Illinois, along with 49 other attorneys general, has reached a settlement with software company Blackbaud concerning its data security practices and response to a 2020 data breach that exposed the personal information of millions of consumers across the United States. Under the settlement, Blackbaud has agreed to overhaul its data security and breach notification practices and make a $49.5 million payment to states. Illinois will receive $2.28 million from the settlement.

Blackbaud provides software to various nonprofit organizations, including charities, higher education institutions, K-12 schools, health care organizations, religious organizations and cultural organizations. Blackbaud's customers use Blackbaud's software to connect with donors and manage data about their constituents, including contact and demographic information, Social Security numbers, driver's license numbers, financial information, employment and wealth information, donation history and protected health information. This type of highly-sensitive information was exposed during the 2020 data breach, which impacted over 13,000 Blackbaud customers and their respective consumer constituents.

"Thousands of Illinoisans were affected by Blackbaud's data breach," Raoul said. "Our investigations led to meaningful reforms in the way data is handled, protecting consumers from future exposure and ensuring that if there is a future breach, consumers are properly informed and assistance is provided."

Today's settlement resolves allegations by Raoul and the attorneys general that Blackbaud violated state consumer protection laws, breach notification laws, and HIPAA by failing to implement reasonable data security and remediate known security gaps, which allowed unauthorized persons to gain access to Blackbaud's network.

The attorneys general also alleged that Blackbaud failed to provide its customers with timely, complete or accurate information regarding the breach, as required by law. As a result of

Blackbaud's actions, and delayed notification, some of Blackbaud's customers may have been confused as to whether they were required to notify their own customers.

Under the settlement, Blackbaud has agreed to strengthen its data security and breach notification practices going forward by implementing:

- Personal information safeguards and controls requiring total database encryption and dark web monitoring.
- Specific security requirements with respect to network segmentation, patch management, intrusion detection, firewalls, access controls, logging and monitoring, and penetration testing.
- Breach response plans to prepare for and more appropriately respond to future security incidents and breaches, including adhering to breach notification requirements under state law and HIPAA.
- Breach notification provisions that require Blackbaud to provide appropriate assistance to its customers and support customers' compliance with applicable notification requirements in the event of a breach.
- Security incident reporting to the CEO and board, enhanced employee training, and appropriate resources and support for cybersecurity.
- Third-party assessments of Blackbaud's compliance with the settlement for seven years.

The attorneys general of Indiana and Vermont co-led the multistate investigation, assisted by the executive committee consisting of Attorney General Raoul and the attorneys general of Alabama, Arizona, Florida and New York. These attorneys general were joined in the settlement by Alaska, Arkansas, Colorado, Connecticut, Delaware, the District of Columbia, Georgia, Hawaii, Idaho, Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland, Massachusetts, Michigan, Minnesota, Mississippi, Missouri, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New Mexico, North Carolina, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Carolina, South Dakota, Tennessee, Texas, Utah, Virginia, Washington, West Virginia, Wisconsin and Wyoming.

Bureau Chief Beth Blackston, Chief Privacy Officer Matt Van Hise, Privacy Counsel Carolyn Friedman and Assistant Attorney General Andrew Hong handled today's settlement for Raoul's Consumer Fraud Bureau.