Date of Hearing: January 14, 2020

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Ed Chau, Chair
AB 499 (Mayes) – As Amended April 11, 2019

SUBJECT: Personal information: social security numbers: state agencies

SUMMARY: This bill would prohibit a state agency from sending any outgoing mail that contains an individual's full social security number (SSN), unless federal law requires inclusion of the full SSN, and would require each state agency to report to the Legislature when and why it mails documents that contain individuals' full social security numbers. Specifically, **this bill would**:

1) Beginning January 1, 2023, prohibit a state agency from sending any outgoing mail that contains an individual's full SSN unless, under particular circumstances, federal law requires the inclusion of the full SSN.

2) Require each state agency, on or before September 1, 2020, to report to the Legislature when and why it mails documents that contain individuals' full SSNs.

3) Until January 1, 2024, require a state agency that, in its estimation, is unable to comply with the prohibition on mailing full SSNs to submit an annual corrective action plan to the Legislature until it complies with the above provisions.

4) Require a state agency that is not in compliance with the prohibition on mailing full SSNs to offer to provide appropriate identity theft prevention and mitigation services to any individual, at no cost to the individual, to whom it sent mail that contained the individual's full SSN, as specified.

EXISTING LAW:

1) Prohibits any state agency from sending any outgoing United States mail to an individual that contains personal information about that individual, including, but not limited to, the individual's SSN, telephone number, driver's license number, or credit card account number, unless that personal information is contained within sealed correspondence and cannot be viewed from the outside of that sealed correspondence. (Gov. Code Sec. 11019.7.)

2) Prohibits a person or entity from printing an individual's SSN on any materials that are mailed to the individual, unless state or federal law requires the SSN to be on the document to be mailed. However, SSNs may be included in applications and forms sent by mail, including 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 SSN. (Civ. Code Sec. 1798.85(a)(5).)

FISCAL EFFECT: Unknown

COMMENTS:

1) **Purpose of this bill**: This bill seeks to protect California residents from identity theft by, among other things, prohibiting state agencies from sending any mail to an individual

containing their full SSN, unless a full SSN is required by federal law. This bill is author-sponsored.

2) **Author's statement**: According to the author:

> It goes without saying that an individual's Social Security Number is one of the most important pieces of information an individual should protect. This legislation follows a recommendation by the State Auditor after an investigation into the Employment Development Department (EDD) practice of sending out mail with full Social security numbers. EDD exposed nearly 300 claimants to the risk of identity theft when it inappropriately disclosed their personal information, including SSNs, to other mail recipients. EDD is currently undergoing a system modernization project, which will incorporate a unique identifier to replace SSNs. However, this will not be completed before 2024 and EDD will send approximately 70 million documents with SSNs during this period. It is also unclear that EDD needs to send SSNs through the mail as the State Auditor could not find any laws expressly requiring them to do so.

3) **Widespread use of SSNs makes the identifier an attractive target for identity thieves**: According to the Social Security Administration, the use of the SSN has expanded significantly since its inception in 1936. Created merely to keep track of the earnings history of U.S. workers for Social Security entitlement and benefit computation purposes, it is now used as a nearly universal identifier. Assigned at birth, the SSN enables government agencies to identify individuals in their records and allows businesses to track an individual's financial information. Unfortunately, this universality has led to abuse as the SSN is a key piece of information used to commit identity theft. The Federal Trade Commission estimates that as many as 9 million Americans have their identities stolen each year. (Puckett, *The Story of the Social Security Number* Social Security Bulletin, Vol. 69, No. 2, 2009.)

   For decades, California residents have benefited from laws protecting SSNs from disclosure by the private sector and government agencies. By way of example, SB 458 (Peace, Ch. 685, Stats. 1998) prohibited state agencies from sending any correspondence to an individual that contains personal information about that individual (*e.g.*, social security number, driver's license number, telephone number, or credit card account number) unless the correspondence is sealed. Additionally, since 2002, California has restricted the use and display of SSNs by private actors (*see* SB 168 (Bowen, Ch. 720, Stats. 2001)) by prohibiting companies and persons from engaging in certain activities, such as:

   - posting or publicly displaying SSNs;
   - printing SSNs on cards required to access the company's products or services;
   - requiring people to transmit an SSN over the internet unless the connection is secure or the number is encrypted;
   - requiring people to log onto a website using an SSN without a password; or,
   - printing SSNs on anything mailed to a customer unless required by law or the document is a form or application.

Yet despite states like California regulating the use and disclosure of SSNs, continues. In September 2005, the United States Government Accountability Office issued a report entitled, *Social Security Numbers: Federal and State Laws Restrict Use of SSNs, yet Gaps Remain*. The report found that "SSN use is widespread. Agencies at all levels of government frequently collect and use SSNs to administer their programs, verify applicants' eligibility for services and benefits, and perform research and evaluations of their programs. Although some government agencies are taking steps to limit the use and display of SSNs, these numbers are still available in a variety of public records held by states, local jurisdictions, and courts[.]"

After widespread media coverage of California's Employment Development Department (EDD) printing full SSNs on correspondence to millions of Californians in 2015, EDD claimed it would begin to redact SSNs on 75 percent of all mailed documents. In a recent report regarding EDD's privacy protection practices when mailing documents to its customers, the State Auditor concluded that "[a]lthough EDD has undertaken efforts since 2015 to reduce the amount of mail it sends to claimants that include full SSNs, its efforts have been insufficient." Specifically, the State Auditor found that "EDD likely sent more than 17 million pieces of mail containing full Social Security numbers (SSNs) to a total of more than a million people in fiscal year 2017–18 [and that] several of the security incidents […] reviewed from 2015 through 2018 showed that EDD exposed nearly 300 claimants to the risk of identity theft when it inappropriately disclosed their personal information, including SSNs, to other mail recipients." (The full report (hereinafter "Report") may be found online at <http://www.auditor.ca.gov/pdfs/reports/2018-129.pdf> [as of Jan. 7, 2020].)

Ultimately, the State Auditor found that EDD should take near-term measures to protect its claimants better, and made several recommendations to that effect. This bill would codify a number of those recommendations for all state agencies.

4) **Prohibits the mailing of full SSNs to individuals unless required by federal law**: This bill would prohibit, beginning January 1, 2023, a state agency from sending any outgoing US mail to an individual that contains the individual's full SSN, unless federal law requires the inclusion of a full SSN. This prohibition is taken directly from the State Auditor's report which provides that "[b]ecause other state agencies may mail full SSNs to Californians, and because this practice—regardless of the agency involved—exposes individuals to the risk of identity theft, the Legislature should amend state law to require all state agencies to develop and implement plans to stop mailing documents that contain full SSNs to individuals by no later than December 2022, unless federal law requires the inclusion of full SSNs." (*See* Report at p 22.)

A similar prohibition was contained in SB 447 (DeSaulnier, 2012), which was vetoed by Governor Brown who argued that this prohibition "would hinder the ability of state agencies to promptly and accurately provide information to run essential programs." Arguably, many factors have changed since Governor Brown vetoed that bill eight years ago, thereby justifying the reconsideration of this prohibition by the Legislature. For example, since 2012 many state agencies have updated their privacy practices and means of correspondence in ways that ensure full SSNs are no longer being mailed. Specifically, as more agencies have embraced "paperless" communication, mailing correspondence has become rarer. Additionally, some agencies now issue unique identifiers in lieu of using an SSN, as recommended by California's Office of Privacy Protection (OPP) as early as 2008. Further,

as discussed more below, this bill is distinct from SB 447 in that a delayed implementation date will give state agencies that are still using full SSNs in mailed correspondence time to sufficiently prepare to implement the new law.

5) **Delayed implementation combined with reporting requirements gives state agencies time to update privacy practices and seek statutory amendments if necessary**: Beginning on or before September of this year, this bill would require each state agency to report to the Legislature when and why it mails individuals' full SSNs. Further, this bill would require any agency that, in its estimation, cannot cease mailing full SSNs to individuals by January 1, 2023, to provide to the Legislature an annual correction plan until it can stop mailing full SSNs. Similar to the prohibition discussed in Comment 4 above, these requirements are based on recommendations by the State Auditor in the Report. Specifically, the Report provides:

> To ensure that state agencies sufficiently prepare to implement this new law, the Legislature should also require that, by September 2019, they submit to it a report that identifies the extent to which their departments mail any documents containing full SSNs to individuals. If any agency determines that it cannot reasonably meet the December 2022 deadline to stop including full SSNs on mailings to individuals, the Legislature should require that starting in January 2023, the agency submit to it and post on the agency's website an annual corrective action plan that contains, at a minimum, the following information:
>
> - The steps it has taken to stop including full SSNs on mailed documents.
> - The number of documents from which it has successfully removed full SSNs and the approximate mailing volume that corresponds to those documents.
> - The remaining steps that it plans to take to remove or replace full SSNs it includes on mailed documents.
> - The number of documents and approximate mailing volume that it has yet to address.
> - The expected date by which it will stop mailing documents that contain full SSNs to individuals.

By requiring state agencies to report on specific privacy practices, this bill should not only aid those agencies in preparing to comply with the prohibition in this bill, but will also arguably give the Legislature valuable information that is necessary for this body to appropriately regulate state agencies who may be putting the privacy of California residents at risk and needlessly increasing their exposure to identity theft. At the same time, reports to the Legislature are generally available to the public. Thus, the reporting requirement in this bill would create a public list of state agencies that continue to send full SSNs, which could inform individuals planning on committing identity theft about specific pieces of mail to intercept from claimants. Accordingly, as this bill moves through the legislative process, the author may wish to consider an alternative reporting requirement whereby information that may create security risks is not available to the general public.

Staff additionally notes that this bill, which was amended last April, requires state agencies to report to the Legislature by September 1, 2020. Because the bill, if approved by the Legislature and signed by the Governor, will not go into effect until January 1, 2021, a technical amendment is needed to ensure state agencies are capable of compliance. The following amendment would change the date the reports are due to the Legislature to September 1, 2021.

Author's amendment:

On Page 3, line 11, strike "2020" and insert "2021"

Further, due to timing contraints, should this Committee approve the bill, this amendment will need to be processed by the Assembly Appropriations Committee.

6) **Requires that identity theft prevention and mitigation services be offered to individuals whose SSN has been improperly disclosed**: This bill would require any state agency that continues to send outgoing mail with full SSNs after January 1, 2023, to offer to provide at least one year of appropriate identity theft prevention and mitigation services to any individual whose full SSN was impermissibly mailed, along with all information necessary to take advantage of the offer.

A similar requirement can be found within California's data breach notification law. Specifically, businesses or persons who own or license computerized data that includes personal information are required to disclose data breaches to the persons whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person. Additionally, if the person or business providing the notification was the source of the breach, they must also offer to provide identity theft prevention and mitigation services to the affected person, as specified. (*See* Civ. Code Sec. 1798.82.) Staff notes that this requirement under existing law is imposed only on private actors, not state agencies. That said, this Committee has approved efforts in the past that would have required government entities to extend identity theft and mitigation services to individuals affected by government data breaches. (*See* AB 241 (Dababneh, 2017).)

7) **Prior legislation**: SB 447 (DeSaulnier, 2012) would have prohibited a state agency from sending any communication to any individual that contains the full SSN of that individual unless required by federal law. SB 447 was vetoed by Governor Brown, who argued that this prohibition "would hinder the ability of state agencies to promptly and accurately provide information to run essential programs."

SB 458 (Peace, Ch. Stats. 1998) *See* Comment 3.

REGISTERED SUPPORT / OPPOSITION:

Support

None on file

Opposition

None on file

Analysis Prepared by: Nichole Rocha / P. & C.P. / (916) 319-2200