Date of Hearing: June 14, 2022

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Jesse Gabriel, Chair
SB 1001 (Min) – As Amended March 16, 2022

SENATE VOTE: 39-0

SUBJECT: California Cybersecurity Integration Center: consumer protection: credit reporting

SUMMARY: This bill would require the California Cybersecurity Integration Center (Cal-CSIC) to submit a report to the Legislature on the feasibility and benefits of requiring credit reporting bureaus and lenders to implement new information security tactics that protect consumers from financial fraud, including specified information, on or before December 31, 2023. Specifically, **this bill would**:

1) Require Cal-CSIC, on or before December 31, 2023, to submit to the Legislature a report on the feasibility and benefits of requiring credit reporting bureaus and lenders to implement new information security tactics that protect consumers from financial fraud.

2) Specify that the report pursuant to 1), above, shall include, but not be limited to, an assessment of the feasibility and benefits of utilizing all of the following tactics:

   - Requiring credit reporting bureaus or lenders to use multifactor authentication each time a new line of credit is opened or a credit report is accessed.

   - Utilization of statewide alternatives to social security numbers (SSNs) as authenticators in determining an individual's identity, including a Social Security Number Plus (SSN+), a mobile driver's license, or other proposals that may be promising.

   - Requiring credit reporting bureaus or lenders to accept alternatives to SSNs as authenticators in determining an individual's identity.

3) Require the report submitted pursuant to 1), above, to be submitted in compliance with existing laws pertaining to the submission of reports to the Legislature.

4) Provide that the provisions of the bill are repealed on January 1, 2027.

EXISTING LAW:

1) Establishes, within the office of the Governor, the Office of Emergency Services (CalOES), with responsibility for the state's emergency and disaster response services for natural, technological, or man-made disasters and emergencies, including responsibility for activities necessary to prevent, respond to, recover from, and mitigate the effects of emergencies and disasters to people and property. (Gov. Code Sec. 8585(a) and (e).)

2) Tasks CalOES with establishing and leading Cal-CSIC, comprised of representatives from specified state and federal agencies and offices, with the primary mission of reducing the likelihood and severity of cyber incidents that could damage California's economy, its critical infrastructure, or public and private sector computer networks in our state; and

provides that Cal-CSIC shall serve as the central organizing hub of state government's cybersecurity activities and coordinate information sharing with local, state, and federal agencies, tribal governments, utilities and other service providers, academic institutions, and nongovernmental organizations. (Gov. Code Sec. 8586.5(a).)

3) Tasks Cal-CSIC with developing a statewide cybersecurity strategy, informed by recommendations from the California Task Force on Cybersecurity and in accordance with state and federal requirements, standards, and best practices, to improve how cyber threats are identified, understood, and shared in order to reduce threats to California government, businesses, and consumers; and specifies that the strategy shall also, among other things, standardize implementation of data protection measures. (Gov. Code Sec. 8586.5(c).)

4) Requires a business that owns, licenses, or maintains personal information (PI) about a California resident to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the PI from authorized access, destruction, use, modification, or disclosure; and requires a business that discloses PI about a California resident pursuant to a contract with a nonaffiliated third party to require by contract that the third party implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the PI from unauthorized access, destruction, use, modification, or disclosure. (Civ. Code Sec. 1798.81.5(b) and (c).)

5) Requires any agency, person, or business that owns or licenses computerized data that includes personal information (PI) to disclose a breach of the security of the system, as defined, to any California resident whose unencrypted PI, or encrypted PI along with an encryption key or security credential, was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as specified. (Civ. Code Secs. 1798.29(a) and (c); 1798.82(a) and (c).)

6) Prohibits any state agency from sending any outgoing United States mail to an individual that contains PI 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 PI is contained within sealed correspondence and cannot be viewed from the outside of that sealed correspondence. (Gov. Code Sec. 11019.7(a).)

7) Provides that, notwithstanding any other law, commencing on or before January 1, 2023, a state agency shall not send any outgoing United States mail to an individual that contains the individual's SSN unless the number is truncated to its last four digits. (Gov. Code. Sec. 11019.7(b).)

8) Requires that a report required or requested by law to be submitted to the Members of either house of the Legislature generally, instead be submitted as a printed copy to the Secretary of the Senate, as an electronic copy to the Chief Clerk of the Assembly, and as an electronic or printed copy to the Legislative Counsel, as specified. (Gov. Code Sec. 9795.)

9) Requires that a bill that would require a state agency to submit a report on any subject to either house of the Legislature generally, a committee or office of either house of the Legislature, or the Legislative Counsel Bureau, include a provision that repeals the reporting requirement, or makes the requirement inoperative, no later than a date four years following

the date upon which the bill becomes operative, or four years after the due date of any report required every four or more years. (Gov. Code Sec. 10231.5(a).)

FISCAL EFFECT: According to the Senate Appropriations Committee, "[CalOES] anticipates total costs of approximately $3.50 million (General Fund) [including a] one-time cost of $1.40 million for a consulting contract over a two-year period [and an annual] cost of %1.05 million for four limited term positions for a two-year period."

COMMENTS:

1) **Purpose of this bill**: This bill seeks to improve information security practices in the consumer credit reporting and lending industries and to protect against financial fraud by requiring Cal-CSIC to explore, and report to the Legislature on, the feasibility and benefits of requiring specified security practices by credit reporting bureaus and lenders. This bill is author-sponsored.

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

> SB 1001 will provide the government with needed data on possible solutions they can use in partnership with credit reporting bureaus to protect consumers from identity crime. From multi-factor authentication to alternative authenticators, there are multiple crime prevention tools at our fingertips. This bill promotes comprehensive evaluation of cyber protections that will ultimately protect consumers from needless identity theft attacks in the future.

3) **Data breaches, credit, and financial fraud**: Recent years have seen dramatic increases in both the scope and frequency of data breaches, in which the PI of individuals is compromised. These breaches span both the public and private sector, and can have far-reaching consequences, including invasions of privacy and identity theft leading to financial fraud. Once enough factors of an individual's PI are compromised, identity thieves can effectively present themselves as that individual for the purpose of creating new bank accounts, registering new credit cards, utilities, and wireless telephone accounts, utilizing the victim's insurance, taking out loans at the expense of the victim, and draining or extravagantly spending from the victim's existing accounts. For a victim of this type of financial fraud, the lasting effects can be catastrophic, resulting in dire financial circumstances and often irreversible damage to the victim's credit rating.

   According to the Federal Trade Commission's (FTC) "Consumer Sentinel Network Data Book 2020," the FTC received 1,387,615 identity theft complaints in 2020 alone, more than doubling the 2019 total of 650,523.[1] California accounted for more of these reports than any other state, amounting to over 10% of all reports nationwide. In 2020, the Federal Bureau of Investigation's Internet Crime Complaint Center (FBI IC3) received "a record number of complaints from the American public []: 791,790, with reported losses exceeding $4.1 billion. This represents a 69% increase in total complaints from 2019." According to the FBI IC3 2021 report, California leads the nation by a staggering margin in both the number of

[1] Federal Trade Commission "Consumer Sentinel Network Data Book 2020", Feb. 2021, https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2020/csn_annual_data_book_2020.pdf [as of Jun. 12, 2022].

victims of internet crime and in the estimated costs experienced by the victims, with nearly 50% more victims and over twice the costs compared to the next closest states, respectively.[2] In part, this sizable increase in the rate of identity theft likely resulted from the rapid pandemic-driven shift to online services in contexts that would have otherwise warranted in-person identity verification.

In part, however, this increase may have been a culmination of sorts resulting from a decade rife with data breaches in which sensitive identifying and financial information was compromised. Most notable among these breaches was the 2017 breach of Equifax, one of the largest credit reporting agencies in the United States, which resulted in the unauthorized disclosure of PI concerning nearly half of all Americans. Almost 99% of these unauthorized disclosures included the SSN of the affected individual. As the Electronic Privacy Information Center (EPIC) describes:

> Equifax, one of the three largest consumer credit reporting agencies in the United States, announced in September 2017 that its systems had been breached and the sensitive personal data of 148 million Americans had been compromised. The data breached included names, home addresses, phone numbers, dates of birth, social security numbers, and driver's license numbers. The credit card numbers of approximately 209,000 consumers were also breached. The Equifax breach is unprecedented in scope and severity. There have been larger security breaches by other companies in the past, but the sensitivity of the personal information held by Equifax and the scale of the problem makes this breach unprecedented.

A 2018 Washington Post article enumerates the magnitude of the breach in greater detail, reporting that a filing by Equifax with the Securities and Exchange Commission (SEC) revealed:

> Beyond the information [discussed in the previous quotation], Equifax said the hackers accessed thousands of images of official documents – such as government-issued IDs – that consumers had uploaded to the company to prove their identity. Photos of as many as 38,000 driver's licenses and 12,000 Social Security or taxpayer ID cards were accessed, according to the SEC filing. More than 3,000 passports were also accessed, the company said.[3]

The Equifax breach was only the latest in a string of breaches that have, in the past decade, compromised PI maintained by credit bureaus and lenders. The size of the breach nonetheless revealed two critical realities that, if left unaddressed, have the potential to further jeopardize the security of consumer PI and expose the public to potential financial fraud: that the widespread use of SSNs to both identify (i.e. specify the identity of) and authenticate (i.e. confirm that the person providing the information is who they say they are) individuals exposes Americans to significant vulnerability to identity theft, and that lapses in

---

[2] Internet Crime Complaint Center, "Internet Crime Report 2021," *Federal Bureau of Investigation*, Mar. 22 2022, https://www.fbi.gov/news/pressrel/press-releases/fbi-releases-the-internet-crime-complaint-center-2021-internet-crime-report, [as of Jun. 12, 2022].

[3] Brian Fung, "145 million Social Security numbers, 99 million addresses and more: Every type of personal data Equifax lost to hackers, by the numbers", *Washington Post*, May 8, 2018, https://www.washingtonpost.com/news/the-switch/wp/2018/05/08/every-type-of-personal-data-equifax-lost-to-hackers-by-the-numbers/ [as of Jun. 12, 2022].

the cybersecurity of credit reporting bureaus can have devastating consequences due to their extensive troves of highly personal information.

To prevent future catastrophic breaches that could further expose Californians to identity theft and financial fraud vulnerability, this bill seeks to engage the expertise of Cal-CSIC to identify potential policies and practices that could be adopted by credit bureaus and lenders in order to strengthen identity verification and minimize reliance on traditional identifiers such as SSN that have at this point been largely compromised. By informing a potential transition to more secure identification and authentication practices in the credit reporting and lending space, this bill aims to mitigate the likelihood of and damage resulting from future breaches of these institutions, and to build resilience against the otherwise staggering costs of identity theft.

4) **Cal-CSIC**: Acknowledging the pressing cybersecurity issues facing this State, California has in recent years invested heavily in the security of its IT infrastructure. In 2018, the Legislature passed AB 3075 (Berman, Ch. 241, Stats. 2018) which created the Office of Elections Cybersecurity within the Secretary of State, tasked with the primary mission to coordinate efforts between the Secretary of State and local elections officials to reduce the likelihood and severity of cyber incidents that could interfere with the security or integrity of elections. The Budget Act of 2020 (AB 89, Ting, Ch. 7, Stats. 2020) also made substantial investments in cybersecurity, including allocating $11.1 million to various departments to enhance the cybersecurity of the State's critical infrastructure, and $2.9 million to protect patient health records by strengthening cybersecurity throughout the State's public health infrastructure.

   Of relevance to this bill, in 2015, Executive Order B-34-15 required CalOES to establish and lead Cal-CSIC, with the primary mission to reduce the likelihood and severity of cyber incidents that could damage California's economy, critical infrastructure, or public and private sector computer networks. The existence of Cal-CSIC was codified three years later by AB 2813 (Irwin, Ch. 768, Stats. 2018).

   Section 8586.5 of the Government Code details the makeup and mission of Cal-CSIC, specifying that Cal-CSIC shall serve as the central organizing hub of state government's cybersecurity activities and shall coordinate information sharing with local, state, and federal agencies, tribal governments, utilities and other service providers, academic institutions, and nongovernmental organizations. Pursuant to that code section, Cal-CSIC is comprised of representatives from several state and federal agencies related to and directly affected by cybersecurity functions. Specifically, Cal-CSIC consists of representatives from the following organizations: CalOES; the Office of Information Security; the State Threat Assessment Center; the Department of the California Highway Patrol; the Military Department; the Office of the Attorney General; the California Health and Human Services Agency; the California Utilities Emergency Association; the California State University; the University of California; the California Community Colleges; the United States Department of Homeland Security; the United States Federal Bureau of Investigation; the United States Secret Service; the United States Coast Guard; and other members designated by the Director of Emergency Services. Together, this membership provides for both an intricate and expansive network for sharing information related to cybersecurity threats, and for a body with profound and diverse expertise related to cybersecurity strategy.

In addition to threat assessment and cyber incident response duties, Cal-CSIC is also tasked with developing a statewide cybersecurity strategy, informed by recommendations from the California Task Force on Cybersecurity, which was itself established by a directive of Governor Brown as "a statewide partnership comprised of key stakeholders, subject matter experts, and cybersecurity professionals from California's public sector, private industry, academia, and law enforcement [to serve] as an advisory body to the State of California Senior Administration Officials in matters related to cybersecurity."[4] Statute provides that the strategy shall be developed to improve how cyber threats are identified, understood, and shared in order to reduce threats to California government, businesses, and consumers, and that the strategy shall also strengthen cyber emergency preparedness and response, standardize implementation of data protection measures, enhance digital forensics and cyber investigative capabilities, deepen expertise among California's workforce of cybersecurity professionals, and expand cybersecurity awareness and public education. (Gov. Code Sec. 8586.5(c).)

This bill seeks to capitalize on the substantial expertise among the Cal-CSIC's membership in order to identify best practices and policy solutions that could better protect Californians from financial fraud. The infamous Equifax data breach in 2017 demonstrated the remarkable breadth of consequences that can result from data insecurity among credit bureaus and lenders, and highlighted the shortcomings of the use of SSNs as singular authenticators and identifiers for verifying identity. In light of these revelations, this bill directs the expertise of Cal-CSIC toward exploring the feasibility and benefits of various practices that could improve the security of PI held by credit bureaus and lenders and help defend against identity theft and fraud. The bill requires the findings of these explorations to be reported to the Legislature to inform future policy.

5) **Bill provides for the exploration of several options for protection against financial fraud, but does not require reporting on the downsides of these approaches**: This bill requires Cal-CSIC to submit a report to the Legislature on the feasibility and benefits of requiring credit reporting bureaus and lenders to implement new information security tactics that protect consumers from financial fraud. The bill specifies that the report should, in particular, assess the feasibility and benefits of utilizing the following practices: requiring credit reporting bureaus or lenders to use multifactor authentication each time a new line of credit is opened or a credit report is accessed; utilization of statewide alternatives to SSNs as authenticators in determining an individual's identity including SSN+, a mobile driver's license, "or other proposals that may be promising"; and requiring credit reporting bureaus or lenders to accept alternatives to SSNs as authenticators in determining identity.

Notably, while the bill requires reporting on the "feasibility and benefits" of those tactics, it does not specify that the report should explore potential risks, downsides, costs, or other pitfalls of adopting those practices, and does not require comparative evaluation of those practices relative to other alternatives. Though costs may comprise one aspect of feasibility, arguably the feasibility of a practice generally refers to whether that tactic *can* be implemented, rather than whether it *should*. As such, the construction of the bill's provisions seem to bias the required report in favor of these tactics, should the capacity exist to put them into practice. All of these practices undoubtedly provide certain documented benefits for the

[4] Cybersecurity Task Force, "About", CalOES, https://www.caloes.ca.gov/cal-oes-divisions/cybersecurity-task-force [as of Jun. 12, 2022].

security of PI, and would thus conceivably protect consumers from financial fraud - the report this bill would require is instructed to expound on these benefits. But it is likely that other similarly effective or more effective approaches to protecting PI and preventing financial fraud also exist, making a thorough assessment of the benefits of the tactics weighed against their downsides essential.

For instance, the bill calls for assessment of the feasibility and benefits of mobile driver's licenses, i.e. government-issued credentials that are carried on a mobile device and accessed via a mobile application, a concept which has been considered previously by this Legislature (*see*, e.g., AB 1503 (Santiago, 2021)). For mobile driver's licenses, there are numerous benefits for protecting against financial fraud, including making identity verification more convenient and facilitating identity verification for services acquired online (e.g. opening lines of credit), and significant feasibility considerations, such as the development of an authentication infrastructure by the State. In addition to these considerations that the report, as required, would contemplate, however, there are also significant privacy and security considerations that the report could potentially overlook, including Fourth Amendment and government surveillance concerns, the possibility for the collection of extraneous data when using a mobile application to access or present the license, and the vulnerability to hacking depending on how the infrastructure is constructed (for a more in-depth analysis of some of these considerations re mobile driver's licenses, refer to this Committee's analysis of AB 1503 (Santiago, 2021)).

Accordingly, should this bill pass out of this Committee, as the bill moves through the Legislative process, the author may wish to consider clarifying that the report should explore both the pros *and* the cons of these approaches, in addition to their feasibility.

6) **SSN+ does not appear to be a well-established or well-defined concept based on a dearth of relevant primary sources**: This bill requires that the report assess the feasibility and benefits of utilizing SSN+ as an alternative to SSNs to authenticate an individual's identifying information, but it is not entirely clear to what this requirement refers. While multifactor authentication and mobile driver's licenses are well precedented, with a cursory online search yielding several descriptions and analyses of these concepts, SSN+ seems to be less established. Extensive online research by committee staff yielded only one description of an alternative identity authenticator called "SSN+", which was found in a September 15, 2020 blog post on the website of the data security and identity verification company Spruce entitled "Reimagining the Social Security Number."[5] As that post describes:

> *The process would start with an individual voluntarily enrolling to receive an SSN+ package (as we're calling it).* This would require first passing the appropriate levels of identity proofing, not dissimilar from those necessary in the existing process of SSN card replacement or enrollments in other comparable identity documentation programs. […]
>
> Once equipped with an SSN+ package, a user can approach the institutions currently using their SSN as a knowledge-based authenticator and register their account's support for SSN+ improved authentication. This re-enrollment involves little more than being presented with an additional challenge that only someone with the corresponding SSN+

[5] "Reimagining the Social Security Number," *Spruce*, Sep. 15, 2020, https://blog.spruceid.com/reimagining-the-social-security-number/ [as of Jun. 11, 2022].

> package could correctly answer. Each new authentication challenge thereafter would similarly require a new SSN+ challenge.[6]

Though the blog post goes on to describe possible implementations of SSN+ in more detail, and to extoll their respective virtues, the lack of readily accessible resources concerning the SSN+ model may complicate the process of comprehensively assessing its feasibility and benefits. It may therefore be beneficial, as the bill moves through the Legislative process, for the author to consider substituting a better-defined and more generally accessible concept in specifying an alternative to SSN to be explored by the report, such as that of decentralized identifiers (DIDs).

Despite these technical complications, this bill nonetheless seems prudent in its approach to policymaking with respect to cybersecurity and financial fraud in the credit reporting and lending space. Rather than requiring adoption of particular tactics by credit bureaus and lenders outright, the bill instead seeks the advice and expertise of Cal-CSIC in determining which available options would be most effective, and most feasible, for protecting consumers against financial fraud. This approach seems to appropriately acknowledge both the complexity and the importance of the issue.

7) **Related legislation**: SB 844 (Min) would require Cal-CSIC to submit an annual report to the Legislature on the progress and usage of federal cybersecurity grants issued by the United States Department of Homeland Security pursuant to the State and Local Cybersecurity Improvement Act of 2021.

   SB 892 (Hurtado) would require CalOES to develop, propose, and adopt optional reporting guidelines for companies and cooperatives in the food and agriculture industry and entities in the water and wastewater systems industry if they identify a significant and verified cyber threat; and would require CalOES and Cal-CSIC to prepare and submit a multiyear outreach plan to assist the food and agriculture and water and wastewater sectors in their efforts to improve cybersecurity, and evaluate options for providing grants or other funding to those sectors to improve cybersecurity preparedness.

   AB 2135 (Irwin) would require state agencies that do not fall under the direct authority of the Governor to adopt and implement certain information security and privacy policies, standards, and procedures meeting specified federally-established criteria, and would require those agencies to perform a comprehensive independent security assessment every two years for which they may contract with the Military Department or a qualified responsible vendor.

   AB 2190 (Irwin) would require that the chief of the Office of Information Security submit an annual statewide information security status report including specified information to the Assembly Committee on Privacy & Consumer Protection and to the Senate Governmental Organization Committee beginning no later than January 2023.

   AB 2355 (Salas) would require local educational agencies (LEAs) to report cyberattacks impacting more than 500 pupils or personnel to Cal-CSIC, and would require Cal-CSIC to

---

[6] *Ibid.;* Emphasis added.

track and annually report to the Legislature on cyberattacks and data breaches affecting LEAs.

8) **Prior legislation**: AB 56 (Salas, Ch. 510, Stats. 2021) comprehensively regulates the Employment Development Department (EDD), by, among other things, codifying various recommendations from the State Auditor related to EDD, including requiring EDD to provide access to and pay for identity theft monitoring for any individual who receives outgoing United States mail from EDD that contains a full SNN, and requiring any request for claimant PI from EDD to be made in accordance with the most recent federal standards promulgated by the National Institute of Standards and Technology.

   AB 1503 (Santiago, 2021) would have established a pilot program to evaluate the use of optional mobile or digital alternatives to driver's licenses and identification cards, as specified. This bill was held under submission on the Suspense File in the Assembly Appropriations Committee.

   AB 89 (Ting, Ch. 7, Stats. 2020) *see* Comment #4.

   AB 2813 (Irwin, Ch. 768, Stats. 2018) *see* Comment #4.

   AB 3075 (Berman, Ch. 241, Stats. 2018) *see* Comment #4.

REGISTERED SUPPORT / OPPOSITION:

Support

None on file

Opposition

None on file

Analysis Prepared by: Landon Klein / P. & C.P. / (916) 319-2200