SENATE JUDICIARY COMMITTEE
Senator Thomas Umberg, Chair
2023-2024 Regular Session

SB 591 (Min)
Version: March 22, 2023
Hearing Date: April 18, 2023
Fiscal: Yes
Urgency: No
CK

SUBJECT

California Cybersecurity Integration Center: consumer protection: credit reporting

DIGEST

This bill requires the California Cybersecurity Integration Center to issue a report on the feasibility and benefits, risks, and costs of, requiring credit reporting bureaus and lenders to implement certain information security measures.

EXECUTIVE SUMMARY

Within the Office of Emergency Services (OES), the California Cybersecurity Integration Center (Cal-CSIC) stands to reduce the likelihood and severity of cyber incidents that could damage California's economy, its critical infrastructure, or public and private sector computer networks within the state.

In recent years, California has seen a spike in identity theft and other critical threats to the security of personally identifying information. The impact this has on the lives of Californians, and particularly their financial wellbeing, cannot be understated.

This bill requires Cal-CSIC to develop and submit a report analyzing the feasibility and benefits of placing legal requirements on credit reporting bureaus and lenders to adopt new information security measures. The goal is to protect consumers from financial fraud. The report is required to include assessments of specified methods, including the use of multifactor authentication and the acceptance of alternative authenticators to social security numbers. The report deadline is December 31, 2025.

The bill is author sponsored. There is no known support or opposition. This bill passed out of the Senate Governmental Organization Committee on a vote of 15 to 0.

PROPOSED CHANGES TO THE LAW

Existing law:

1) Establishes Cal-CSIC, within the Office of Emergency Services (OES), to reduce the likelihood and severity of cyber incidents that could damage California's economy, critical infrastructure, or computer networks in the state. (Gov't Code § 8586.5.)

2) Requires Cal-CSIC to serve as the central organizing hub of state government's cybersecurity activities and to coordinate information sharing with local, state, and federal agencies, tribal governments, utilities and other service providers, academic institutions, and nongovernmental organizations. (Gov't Code § 8586.5.)

3) Specifies that any report required or requested by law to be submitted by a state or local agency to the Members of either house of the Legislature generally to 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. (Gov't Code § 9795.)

4) Requires a bill that provides for 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, to 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, as enacted, becomes operative or four years after the due date of any report required every four or more years. (Gov't Code § 10231.5.)

This bill:

1) Requires the California Cybersecurity Integration Center, on or before December 31, 2025, to submit to the Legislature a report on the feasibility of, and benefits, risks, and costs of, requiring credit reporting bureaus and lenders to implement new information security tactics that protect consumers from financial fraud, in accordance with the procedures laid out in Government Code Section 9795.

2) Requires the report to include an assessment of the following tactics:
    a) 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;
    b) utilization of statewide alternatives to social security numbers as authenticators in determining an individual's identity; and

c) requiring credit reporting bureaus or lenders to accept alternatives to social security numbers as authenticators in determining an individual's identity.

3) Provides that it is repealed as of January 1, 2028, pursuant to Government Code Section 10231.5.

COMMENTS

1. Cybersecurity: The incidence and consequences of data breaches & identity theft

According to the Federal Trade Commission's (FTC) "Consumer Sentinel Network Data Book 2020," people filed more reports about identity theft, in its various forms, than any other complaint in 2020.[1] Nationwide, identity theft has dramatically increased. Ten years ago, the FTC reported a little over 250,000 identity theft complaints. That number jumped to 650,523 in 2019. However, in 2020 alone, the FTC received 1,387,615 such reports from consumers – a doubling of the total in just one year. California accounted for 147,382 of those identity theft reports — more than any other state. For every 100,000 people in California, there were 373 identity theft complaints.

Identity theft victims' information can be misused in numerous ways. One of the most common is the creation of new accounts, including credit card, utility, or wireless telephone accounts. But, victims' information can also be used in other, equally nefarious ways. Once identity thieves have a consumer's personal information, they can drain bank accounts, run up charges on various accounts, get medical treatment on a consumer's health insurance, take out auto loans, or even file a tax return and get a consumer's refund. In some extreme cases, a thief might even give the consumer's name to the police during an arrest, generating false criminal records.

A vast majority of Californians engage in a wide range of activities online. Even before the pandemic forced many people to drastically shift their lives online, 70 percent of people in the state received financial services online, 39 percent telecommuted, 42 percent accessed sensitive health or insurance records online, and 39 percent communicated with doctors.[2] In addition, many companies have realized the financial benefits of collecting as much data on consumers as possible, tracking, storing, and selling the details of our everyday lives. Given the amount of activity online and the massive amount of data being collected and switching hands, concerns about data security have skyrocketed.

---

[1] Federal Trade Commission, *Consumer Sentinel Network Data Book 2020* (February 2021) https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2020/csn_annual_data_book_2020.pdf. All internet citations are current as of April 12, 2023.
[2] Niu Gao & Joseph Hayes, *California's Digital Divide* (February 2021) Public Policy Institute of California, https://www.ppic.org/publication/californias-digital-divide/.

In 2020 alone, estimates suggest that there were over 1000 data breaches resulting in the exposure of over 155 million records.[3] According to the Federal Bureau of Investigation's (FBI) Internet Crime Report, the Internet Crime Complaint Center received "a record number of complaints from the American public in 2020: 791,790, with reported losses exceeding $4.1 billion. This represents a 69% increase in total complaints from 2019."[4] A brief look at a few of the larger breaches illustrates the scope of the problem.

The infamous 2017 breach at Equifax lasted at least several months. "If you have a credit report, there's a good chance that you're one of the 143 million American consumers whose sensitive personal information was exposed in a data breach at Equifax, one of the nation's three major credit reporting agencies."[5] The hackers involved were able to access people's names, Social Security numbers, birth dates, addresses, and driver's license numbers. Over 200,000 consumers also had their credit card numbers stolen. There is evidence that the massive hack of personal information has led to extensive identity theft with the thieves using the stolen information to apply for mortgages, credit cards, and student loans. The information is also being used to tap into bank accounts, to file insurance claims, and to incur massive debts on behalf of affected consumers.

Even before that, a much larger breach occurred in 2013, when hackers accessed Yahoo's email system, gathering data on more than 1 billion users.[6] Several years after the hack, a group began offering the entire database of information for sale on the so-called "dark web" with at least three confirmed buyers paying $300,000 each. The breach was not disclosed by Yahoo until 3 years after it occurred. It came after an earlier breach of 450,000 accounts in 2012 and before a hack in 2014 of 500 million user accounts.

More recently, in 2019, the personal information of over 530 million Facebook users was taken in a breach that exploited a vulnerability in a Facebook feature.[7] The company

---

[3] Joseph Johnson, *Cyber crime: number of breaches and records exposed 2005-2020* (March 3, 2021) Statista, https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/#:~:text=In%202020%2C%20the%20number%20of,%2Dthan%2Dadequate%20information%20security.

[4] Internet Crime Complaint Center, *2020 Internet Crime Report* (March 17, 2021) FBI, https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf.

[5] Seena Gressin, *The Equifax Data Breach: What to Do* (Sep. 9, 2017) Federal Trade Commission, https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do.

[6] Vindu Goel & Nicole Perlroth, *Hacked Yahoo Data Is for Sale on Dark Web* (December 15, 2016) The New York Times, https://www.nytimes.com/2016/12/15/technology/hacked-yahoo-data-for-sale-dark-web.html.

[7] Emma Bowman, *After Data Breach Exposes 530 Million, Facebook Says It Will Not Notify Users* (April 9, 2021) NPR, https://www.npr.org/2021/04/09/986005820/after-data-breach-exposes-530-million-facebook-says-it-will-not-notify-users.

indicated it has decided not to notify the individual users affected, but the information remains publicly available after being posted to an online hacking forum. Major breaches have also occurred more recently, with GEICO having driver's license data on 132,000 customers stolen and a hack of the ParkMobile application resulting in the personal information of 21 million users exposed.[8]

The market for this unlawfully obtained data is lucrative. In fact, some companies are reported to be selling government agencies access to stolen data creating an "end-run around the usual legal processes."[9] Unfortunately, because of the size of its economy and the sheer number of consumers, the data collected and held by California businesses is frequently targeted by cyber criminals, and California accounts for a sizeable share of the nation's data breaches.[10] These security breaches are not harmless. The Attorney General reports that 67 percent of breach victims in the United States were also victims of fraud.

2. Existing laws protecting against data breaches and identity theft

The frequency of data breaches and identity theft in California and the threat it poses underscores the crucial need to enact and enforce statutes protecting against and responding to these breaches, and the fraud and identity theft that can result. California has addressed these issues over the years by requiring specific procedures for notifying individuals of data breaches; requiring certain security procedures and practices to prevent such breaches; and providing a right of action if such requirements are not implemented.

In 2003, California's first-in-the-nation security breach notification law went into effect.[11] Since that time, all but three states have enacted similar security breach notification laws, and governments around the world have or are considering enacting such laws. California's data breach notification law requires any agency, person, or business that owns or licenses computerized data that includes personal information to disclose a breach of the security of the system to any California resident whose unencrypted personal information 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. This notification requirement ensures that residents are made

---

[8] Zack Whittaker, *Geico admits fraudsters stole customers' driver's license numbers for months* (April 19, 2021) TechCrunch, https://techcrunch.com/2021/04/19/geico-driver-license-numbers-scraped/; Joe Marusak, *If you find parking spots with this popular app, your data may have been stolen* (April 16, 2021) Charlotte Observer, https://www.charlotteobserver.com/news/local/article250666434.html.
[9] Joseph Cox, *Police Are Buying Access to Hacked Website Data* (July 8, 2020) Vice, https://www.vice.com/en/article/3azvey/police-buying-hacked-data-spycloud.
[10] California Department of Justice, *California Data Breach Report* (February 2016) https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf.
[11] *See* Civ. Code §§ 1798.29, 1798.82.

aware of a breach, thus allowing them to take appropriate action to mitigate or prevent potential financial losses due to fraudulent activity.

In 2004, AB 1950 (Wiggins, Ch. 877, Stats. 2004) added Section 1798.81.5 to the Civil Code. The stated intent of that section is "to ensure that personal information about California residents is protected" and "to encourage businesses that own, license, or maintain personal information about Californians to provide reasonable security for that information." Section 1798.81.5 currently requires businesses that own, license, or maintain certain personal information to implement and maintain reasonable security procedures and practices, appropriate to the nature of the information, to protect that information from unauthorized access, destruction, use, modification, or disclosure.

Businesses that disclose personal information about a California resident pursuant to a contract with a nonaffiliated third party, that is not covered by the requirement above, must 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 personal information from unauthorized access, destruction, use, modification, or disclosure.[12]

In order to better prepare the state for cyber attacks, Governor Brown established Cal-CSIC by executive order, Executive Order B-34-15. Eventually, in 2018, the center was codified by AB 2813 (Irwin, Ch. 768, Stats. 2018). Cal-CSIC's primary mission is to reduce 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. It serves as the central organizing hub of the state's cybersecurity activities and coordinates information sharing with local, state, and federal agencies, tribal governments, utilities and other service providers, academic institutions, and nongovernmental organizations.

3. Tasking Cal-CSIC to chart paths forward

To address the rise of identity thefts and the growing number of credit crimes, this bill promotes the research of tools to protect consumers from increasingly sophisticated attacks specifically in the credit reporting and consumer lending industry. On or before December 31, 2025, Cal-CSIC is required to submit to the Legislature a report on the feasibility of, and benefits, risks, and costs of, requiring credit reporting bureaus and lenders to implement new information security tactics that protect consumers from financial fraud.

Specifically, the report must include an assessment of the feasibility, benefits, risks, and costs of utilizing the following tactics:

[12] Civ. Code § 1798.81.5.

- 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 as authenticators in determining an individual's identity; and
- requiring credit reporting bureaus or lenders to accept alternatives to social security numbers as authenticators in determining an individual's identity.

According to the author:

> It is no longer a matter of if your identifying information will be stolen, but rather when. Identity theft is on the rise in the United States, as during the COVID-19 pandemic. In 2021, the Federal Trade Commission received nearly 2.8 million identity theft incident reports, which was up from the 2.1 million received the year prior. Identity theft crimes come at a high financial and personal cost to individuals and families, and we must be doing more to research technological protections.
>
> SB 591 will provide the government with much-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.

SB 1001 (Min, 2022) was nearly identical to this bill and it passed both houses of the Legislature. Governor Newsom vetoed the bill, explaining his reasoning in his veto message:

> I am supportive of efforts to improve cybersecurity. Through the budget process, we have substantially increased the capacity of the CalCSIC in recent years, and in October last year, my administration published Cal Secure, the State's first ever multi-year cybersecurity roadmap that addresses critical gaps in the state's information and cybersecurity programs while enabling the state to manage existing and future threats more effectively. However, this bill would require millions of dollars not accounted for in the budget for the research and industry expertise needed to complete the feasibility studies.
>
> With our state facing lower-than-expected revenues over the first few months of this fiscal year, it is important to remain disciplined when it comes to spending, particularly spending that is ongoing. We must prioritize existing obligations and priorities, including education, health care, public safety and safety-net programs.

SUPPORT

None known

OPPOSITION

None known

RELATED LEGISLATION

Pending Legislation:

SB 265 (Hurtado, 2023) requires Cal OES to direct Cal-CSIC to prepare, and Cal OES to submit to the Legislature on or before January 1, 2025, a strategic, multiyear outreach plan to assist critical infrastructure sectors, as defined, in their efforts to improve cybersecurity and an evaluation of options for providing grants or alternative forms of funding to, and potential voluntary actions that do not require funding and that assist, that sector in their efforts to improve cybersecurity preparedness. SB 265 is currently in the Senate Appropriations Committee.

AB 1023 (Papan, 2023) explicitly includes school districts, county offices of education, and charter schools among the specified entities with which Cal-CSIC coordinates information sharing, including cyber threat information. AB 1023 is currently in the Assembly Emergency Management Committee.

Prior Legislation:

SB 844 (Min, Ch. 505, Stats. 2022) requires the California Cybersecurity Integration Center (Cal-CSIC) to create an annual report for four years on all expenditures made by the state within a single fiscal year pursuant to the federal State and Local Cybersecurity Improvement Act.

SB 1001 (Min, 2022) *See* Comment 3.

AB 430 (Grayson, Ch. 265, Stats. 2021) allows the use of a Federal Trade Commission identity theft report, in lieu of a police report, when a victim of identity theft seeks civil protections pursuant to the Rosenthal Fair Debt Collection Practices Act, the Identity Theft Law, and the Penal Code, as specified.

AB 825 (Levine, Ch. 527, Stats. 2021) added "genetic information" to the definition of personal information for purposes of the laws requiring certain businesses to implement and maintain reasonable security procedures and practices to protect personal information they own, license, or maintain. It requires businesses and agencies that maintain personal information to disclose a breach of genetic information.

AB 1391 (Chau, Ch. 594, Stats. 2021) makes it unlawful for a person to sell data, or sell access to data, that the person has obtained or accessed pursuant to the commission of a crime. It further makes it unlawful for a person, who is not an authorized person, to purchase or use data from a source that the person knows or reasonably should know has obtained or accessed that data through the commission of a crime.

AB 2813 (Irwin, Ch. 768, Stats. 2018) *See* Comment 2.

AB 1950 (Wiggins, Ch. 877, Stats. 2004) *See* Comment 2.

PRIOR VOTES:

Senate Governmental Organization Committee (Ayes 15, Noes 0)

****