



PROGRAM MATERIALS

Program #30260

November 16, 2020

Emerging Issues in Cybersecurity & Privacy Law

**Copyright ©2020 by Daniel Marvin, Esq. and Alex D'Amico, Esq.- Morrison Mahoney LLP.
All Rights Reserved.
Licensed to Celesq®, Inc.**

Celesq® AttorneysEd Center
www.celesq.com

**5255 North Federal Highway, Suite 310, Boca Raton, FL 33487
Phone 561-241-1919 Fax 561-241-1969**

Emerging Trends

- Consumers being given more control over PII
- More state statutes requiring data protection and privacy plans
- Ever expanding definition of PII
- Changing standards of care for negligence claims
- Prior breaches at a company giving rise to increased duty
- Economic Harm doctrine losing steam
- Creative Plaintiffs bar
- Enforcement by government agencies growing





SHIELD ACT

Stop Hacks and Improve Electronic Data Security Act

Went fully into effect on **March 21, 2020** and requires:

- Businesses that own or license a New York resident's private information to provide notification to such resident, irrespective of whether the company conducts business in the state
- Breach notification to New York residents when there is an unauthorized access (not just acquisition) of private information
- Businesses to implement "reasonable" safeguards to protect private information.
- Implementation of a data security program setting forth reasonable administrative, technical and physical safeguards





SHIELD ACT

Stop Hacks and Improve Electronic Data Security Act

- No private right of action
- Enforcement by the Attorney General:
 1. May seek restitution from entities that fail to comply with breach notice requirement
 2. May seek injunctive relief from entities that fail to implement reasonable safeguards to protect personal information
- Standard of care for a negligence action?





SHIELD ACT

What will enforcement look like?

- Litigation arising from the Department of Financial Services Regulations (Effective March 1, 2017) may provide a guide
 - The DFS need not prove damages to establish standing—a violation of the regulations is sufficient
 - As an example, on July 21, 2020, the DFS commenced an action against First American Title Insurance Co., alleging violations of six DFS regulations in connection with a breach that exposed 885 million mortgage records
 - The DFS is purportedly seeking \$1,000 per record.





Connecticut Insurance Data Security Law

Conn. Gen. Stat. § 38a-38

On June 4, 2019, the Connecticut General Assembly enacted the Insurance Data Security Law ("Act") which becomes effective October 1, 2020. The Act establishes standards applicable to licensees of the Connecticut Insurance Department for data security, the investigation of a cybersecurity event, and notification to the Department of such event.

- Based on NAIC Model Law
- Based on NY DFS Cybersecurity Regulation (gold standard).

Information Security Program: Licensees must develop, implement and maintain a comprehensive written information security program ("ISP") that complies with the requirements of Conn. Gen. Stat. § 38a-38(c) not later than **October 1, 2020.**





Connecticut Insurance Data Security Law

Conn. Gen. Stat. § 38a-38

- Due diligence in selecting third-party service providers.
- Annual Certification by Domestic Insurers (some exceptions, such as small licensees and HIPAA compliant entities).
- Investigation into cybersecurity events.
- Notification to Commissioner.
- Notification to Consumers in compliance with Connecticut's data breach notification law.





Connecticut Insurance Data Security Law

Conn. Gen. Stat. § 38a-38

Third Party Services Providers

- How are vendors dealing with their employees working from home and implementing policies concerning the handling of YOUR data? Reassess risk.
- Understand how YOUR data has been moved to deal with a remote workforce.
- Do your vendor contracts cover increased COVID-19 vendor cybersecurity risks (monitoring connected devices, MFA, application security, remote work policy).
- Require vendors to have WFH policies at least as strong as yours.
 - Level of authentication required to access networks
 - Continuous network monitoring
 - Application security





Connecticut Insurance Data Security Law

Conn. Gen. Stat. § 38a-38

- Secure computer and Internet user authentication protocols (MFA, passwords, etc.)
- Secure access control (restriction of access, encryption, monitoring, firewalls).
- Designation of one or more employees to oversee and maintain security program.
- Identification and assessment of reasonably foreseeable internal and external risks to the security, confidentiality or integrity of electronic or paper PII.
- Evaluation and improvement of effectiveness of safeguards for limiting risks, including employee training, compliance, upgrades and oversight of third-party vendors.
- Development of employee security policies and procedures for the storage of, access to, transport of and transmittal of PII off-premises.





Connecticut Insurance Data Security Law

Conn. Gen. Stat. § 38a-38

- Employee, training Imposition of disciplinary measures on employees
- Prevention of terminated, inactive or retired employees from accessing personal information.
- Reasonable restrictions on physical access to personal information in paper format and storage of such data in locked facilities, storage areas or containers.
- Annual review of practices (or whenever there is a material change in the company's business practices that may affect the security of PII).
- Mandatory post-incident review following any actual or suspected breach of security, and documentation of actions taken in response, including any changes the company makes to its business practices relating to the safeguarding of personal information.



Breach Notification Statutory Amendments – 2020 and Beyond

District of Columbia - Amendments Effective as of June 17, 2020

- **Personal Information** now includes genetic, biometric, and other medical information; Taxpayer numbers, military I.D.'s, and passport numbers; and “[a] username or e-mail address in combination with a password...or data elements...that permit[] access....”
- If more than 50 residents are affected, the **OAG** must be notified.
- HIPAA compliance exemption.



Breach Notification Statutory Amendments – 2020 and Beyond

District of Columbia (continued)

- **Security Requirements** – Reasonable security safeguards, including procedures and practices that are appropriate to the nature of the personal information and the nature and size of the entity or operation must be implemented.
- **“Breach of the security of the system”** – unauthorized **acquisition** of computerized data. Does **NOT** include: (1) unauthorized acquisition of encrypted or redacted data, or (2) when after a reasonable investigation, consultation with the OAG and federal law enforcement agencies, it is determined that **harm will likely not occur**.



Breach Notification Statutory Amendments – 2020 and Beyond

Maine – Amendments Effective July 1, 2020

Added a 30-day notification deadline “after becoming aware of the breach and identifying its scope.”

Vermont - Amendments Effective as of July 1, 2020

Broadens PII to include: (1) username, email address, or any other account holder’s identifying information, in combination with any password or security question and answer that would permit access to an online account; (2) genetic, biometric and other medical information; (3) expanded scope of government I.D. triggering notification.





EU General Data Protection Regulation

International Data Transfers (from an EU country to a non-EU country)

- Permissible if:
 - The country data is transferred to has been approved by the European Commission as having an adequate level of protection; or
 - There are appropriate safeguards and enforceable data subject rights and effective legal remedies for data subjects are available
 - The “appropriate safeguards” may be provided by:
 - A binding agreement between public authorities
 - Binding corporate rules
 - Standard contractual clauses



EU General Data Protection Regulation

European High Court Invalidates the Privacy Shield in “Schrems II” Decision

- The Privacy Shield was a framework designed by the US Department of Commerce and the European Commission
- The Privacy Shield was created after a prior framework, called the “Safe Harbor” was invalidated by the Court of Justice of the E.U. (CJEU) in a lawsuit initiated by Max Schrems
- More than 5,300 companies relied upon the “**Privacy Shield**” agreement
- Schrems sued Facebook in connection with the *still* allegedly insufficient data protection policies under the Privacy Shield
- On July 16, 2020, the CJEU ruled in favor of Schrems, invalidating the Privacy Shield
- However, (for the time being) standard contractual clauses are still a valid mechanism for data transfer



EU General Data Protection Regulation

Top reasons for fines:

- Insufficient technical and organizational measures to ensure information security: €335,159,507
- Insufficient legal basis for data processing: €128,526,632
- Non-compliance with general data processing principles: €17,091,765
- Insufficient fulfilment of data subject (consumer) rights: €9,504,697

Source: GDPR Enforcement Tracker, www.enforcementtracker.com





EU General Data Protection Regulation

Major GDPR Fines:

- British Airways (United Kingdom): € 204,600,000
- Marriott Int'l, Inc (United Kingdom): € 110,390,200
- Google, Inc. (France): € 50,000,000
- TIM (telecommunications operator) (Italy): € 27,800,000



EU General Data Protection Regulation

Total sum of fines per country:

- United Kingdom: € 315,310,200
- Italy: € 57,159,000
- France: € 51,100,000
- Germany: € 26,377,925
- Austria: € 18,070,100
- Sweden: € 7,085,430
- The Netherlands: € 3,490,000



California Consumer Privacy Act of 2018

Took effect on January 1, 2020, dealing with consumer privacy and providing consumers four basic rights related to the collection and use of their personal information:

- The right to know what personal information a business has collected, how it is being used (sold or disclosed), to whom it is being sold or disclosed and the source of the information;
- The right to “opt out” of allowing a business to sell their personal information to third parties;
- The right to have a business delete their personal information; and
- The right to receive equal service and pricing from a business, even if they exercise their privacy rights under the Act.





Attorney General Regulations

- On June 1, 2020, California's Attorney General released Final CCPA Regulations
- The Regulations provide clarity for both consumers and businesses and implement requirements that further the legislative intent of the CCPA.
- Processes for handling Consumer requests must relate in some way to the primary method of communication between the business and its clientele.
 - i.e. – If a business is exclusively online, they only need to provide an email address to customers. All other businesses must provide at least two other methods for submitting requests.





Enforcement

The Office of Attorney General statement from March 19, 2020:

“Right now, we’re committed to enforcing the law upon finalizing the rules or July 1, whichever comes first. We’re all mindful of the new reality created by COVID-19 and the heightened value of protecting consumers’ privacy online that comes with it. We encourage businesses to be particularly mindful of data security in this time of emergency.”

(Made in response to a letter received from influential marketing groups asking for “temporary forbearance” until January 2, 2021)





Enforcement

The Office of Attorney General' statement from July 1, 2020: "Today we begin enforcement of the California Consumer Privacy Act (CCPA), a first-of-its-kind data privacy law in America. We encourage every Californian to know their rights to internet privacy and every business to know its responsibilities. The website of every business covered by the law must now post a link on its homepage that says 'Do Not Sell My Personal Information'. Click on it. Remember, it's your data. You now get to control how it's used or sold."

- Confidential letters of noncompliance went out that same day, targeting multiple industries and business sectors
- They focused on businesses that operated online and neglected to include a "Do Not Sell" link where the AG thought one was necessary
- Targeting was based in part on consumer complaints, including those submitted by social media





Enforcement

What claims have private Consumers brought thus far?

- Data Breach
- Failure to comply with the CCPA notice and opt-out provisions
- Claims under California's Unfair Competition Law

Issues still to be tested

- Does failure to provide effective notice constitute an "unauthorized use" for data breach purposes?
- Does the Federal Arbitration Act override the private right of action guaranteed by the CCPA where there is an arbitration agreement between the business and the consumer?





Overhaul Immanent Already?

The **California Privacy Rights Act of 2020** (CPRA), is a ballot initiative that will significantly amend the CCPA:

- Added definition of “sensitive personal information,” which would be a subset of data within the definition of personal information
- New consumer rights: 1) to correct PI; 2) to know the length of data retention; 3) right to opt-out of advertisers collecting precise geolocation; and 4) the right to restrict the usage of “sensitive personal information”
- Expanded private right of action: extending the scope of liability to include breaches of email addresses and passwords or security questions, if they would allow access to an account and the business fails to maintain reasonable security measures
- Expanded requirements for subject businesses (i.e. a request to delete would force the collector to notify every vendor that it shared the consumer’s information with)
- Creates the California Privacy Protection Agency: the first U.S. State agency dedicated to privacy enforcement



Data Breach Class Actions: Standing

To have Article III Standing to sue in federal court, Plaintiff must demonstrate

- (i) an injury in fact that is
- (ii) concrete and particularized and
- (iii) actual or imminent, not conjectural or hypothetical.

Does a data breach involving a person's PII result in a sufficient injury to give rise to Article III standing?



Data Breach Class Actions: Standing

BLAHOUS v. SARRELL REGIONAL DENTAL CENTER FOR PUBLIC HEALTH (M.D. Ala. Jul. 16, 2020)

WHAT HAPPENED:

Beginning in January 2019, and over the span of several months, hackers continually infiltrated the computer network of Sarrell Regional Dental Center for Public Health, ultimately installing ransomware. Investigations yielded no evidence that the information was copied, downloaded, removed or misused. The plaintiff commenced a class action with both tort and contract claims. Defendants filed a motion to dismiss for lack of standing.

PLAINTIFF'S ALLEGED INJURIES: (1) increased risk of identity theft; (2) costs to mitigate that risk (credit monitoring); (3) overpayment for dental service relating to misrepresentation of data protections; and (4) diminished value of their PII by virtue of its possible exposure



Data Breach Class Actions: Standing

BLAHOUS v. SARRELL REGIONAL DENTAL CENTER FOR PUBLIC HEALTH (continued)

DISTRICT COURT'S RULING: No standing.

The potential for misuse of PII was not grounds to sue the party who failed to protect the data. The court concluded that all alleged injuries were too attenuated to be attributable to the target's failure to secure the data in question.

“The Plaintiffs' claim that they suffered money damages because they paid for services at Sarrell but would not have done so had they known that Sarrell would get hacked later on, is pure applesauce.”



Data Breach Class Actions: Standing

In re BRINKER DATA INCIDENT LITIGATION (MD Fla. 2020)

WHAT HAPPENED:

The plaintiffs alleged that in or around 2018, Brinker International Inc., the parent company of Chili's Bar & Grill, maintained inadequate IT security systems that resulted in hackers stealing their payment card information. The plaintiffs sought, among other things, declaratory and injunctive relief based on the allegation that the information remains stored on Brinker's data systems.

THE ISSUE:

Is the threat of a hacker stealing the current data on Brinker's system, in an attempt to gain access to new credit card information, a sufficient injury for a standing analysis?



Data Breach Class Actions: Standing

In re BRINKER DATA INCIDENT LITIGATION (continued)

DISTRICT COURT'S RULING: dismissed all claims that were based on a future harm

Plaintiff's claims were found to rest on a series of contingencies, all of which could have occurred over the two-year period after the initial incident. The plaintiffs were without standing because there must first be: (1) a second hack; (2) resulting in a credit card processor that automatically updates new cards; (3) the hacker finding a merchant with an agreement with the stolen cards' information; and (4) neither the merchant nor the processor being notified that the cards have been cancelled.

CONSIDER:

- How might this be different a) if a state law like the SHIELD Act applied; or b) there was a private right of action?



Data Breach Class Actions: Standing

BRYANT v. COMPASS GROUP U.S.A., INC. (7th Cir. 2020)

WHAT HAPPENED:

The defendant operated and installed Smart Market vending machines which could only be accessed through the use of a fingerprint scanner. Plaintiff was an employee of an Illinois call center that had installed these vending machines in their cafeteria and sought redress in Illinois state court based on defendant's invasion of her privacy.

STATUTE BACKGROUND:

The Plaintiff brought a claim under the Illinois Biometric Information Privacy Act (BIPA). Pursuant to Illinois Supreme Court precedent, credited by the Seventh Circuit, a statutory claim for a BIPA violation does not require a showing of actual damages to establish standing.



Data Breach Class Actions: Standing

BRYANT v. COMPASS GROUP U.S.A., INC. (continued)

ROLE REVERSAL ON STANDING:

- Defendant removed the case to Federal Court under the Class Action Fairness Act on the basis of diversity and the amount in controversy exceeding five million dollars. Plaintiff moved for the court to remand to state court on the grounds that she did not suffer an injury-in-fact necessary to satisfy Article III standing. (the injury was merely statutory in nature). The district court granted Plaintiff's motion, and Defendant appealed.

CIRCUIT COURT'S RULING: Reversal

- The failure by the defendant to disclose its intentions for collecting biometric information *before* doing so deprives the data subject of the opportunity to make a complete and informed decision about how their PII will be used. The Court ruled that this is a concrete and particularized harm under Article III. The court found that the nature of defendant's violation of BIPA was an invasion of privacy, and it did not require a further showing of tangible injuries.



Data Breach Class Actions: Substantive Issues

In re Marriot Int'l, Inc., 2020 U.S. Dist. LEXIS 30435 (D. Md., Feb. 21, 2020)

WHAT HAPPENED:

- On November 30, 2018, Marriot announced that it had been the target of a breach affecting at least 383 million guests.
- Between July 2014 and September 2018, hackers had access to such PII as names, addresses, phone numbers, and payment card information. In some instances, they were able to view additional information including passport numbers, room preferences, and travel destinations
- The actual target of the breach, Starwood Hotels & Resorts, was acquired by Marriot in September 2016, amid the continuing breach.
- Plaintiffs alleged that the defendants failed to take reasonable steps to secure their data against foreseeable and discoverable cybersecurity risks.



Data Breach Class Actions: Substantive Issues

In re Marriot Int'l, Inc., 2020 U.S. Dist. LEXIS 30435 (continued)

DISTRICT COURT'S RULING: Dismissed negligence claims under Illinois state law for lack of a legal duty to safeguard customers' data. Accordingly, the court did not need to rule on Marriot's argument that the negligence claims should be barred by the **economic loss doctrine**. Nevertheless, the court noted that "data security breach cases do not fit neatly into the paradigm of the cases that led to the adoption of the economic loss doctrine."

'[D]ata security breach cases have very little in common with the products liability cases that launched the economic loss rule, and the policies that underlie that rule . . . do not translate well to the circumstances of a data breach case where it simply cannot be said that the "product"—a hotel room, was in any way defective.'

Is this the beginning of the end for the Economic Loss Doctrine?



Data Breach Class Actions: Substantive Issues

INSURANCE CLAIMS: *Target Corp. v. ACE American Insurance Co.* (D. Minn.)

- Stemming from a December 2013 data breach affecting customers' debit and credit card information, Target was forced to incur more than \$250 million dollars in settlement expenses with a host of stakeholders: affected consumers, major banks, credit card companies, and a coalition of States and D.C.
- In November 2019, Target commenced a lawsuit to recover \$138 million in bank settlement expenses against two of its insurers that had disclaimed coverage under a general liability policy. Target alleged that the policy extended to replacement costs of credit cards since covered "property damage" under the policy included: "the loss of use of tangible property that is not physically injured."



Data Breach Class Actions: Substantive Issues

INSURANCE CLAIMS: *Target Corp. v. ACE American Insurance Co.* (continued)

THE DISPUTE:

- In June 2020, the insurers moved for summary judgement on grounds that there were no damages from loss of use because the financial accounts were still usable, as the cardholder could provide the card number to make purchases.
- In opposition, Target provided the analogy of auto insurance for a motor vehicle accident. Just because the driver can walk from the site of an accident to their destination does not mean they should not receive coverage for repairs of the vehicle.
- This motion is still pending.



Data Breach Class Actions: Substantive Issues

EVIDENTIARY PRIVILEGE: *In re Capital One Customer Data Breach Litigation* (E.D. Va., May 26, 2020)

WHAT HAPPENED: In January 2019, Capital One entered into a Statement of Work (SOW) agreement with cybersecurity consulting firm Mandiant for, among other things, 285 hours of incident response, designating it as a “Business Critical” expense rather than a “Legal” expense. In July 2019, Capital One announced a massive data breach and the first of many lawsuits were filed the next day. Subsequently, Capital One, along with outside counsel, signed a Letter Agreement with Mandiant to perform the services set forth in the SOW. Mandiant’s report, issued on September 4, 2019, highlighted the vulnerabilities that allowed criminal hackers to penetrate Capital One’s security. During discovery, Capital One withheld the report on the basis of attorney-client privilege.



Data Breach Class Actions: Substantive Issues

EVIDENTIARY PRIVILEGE: *In re Capital One Customer Data Breach Litigation* (continued)

DISTRICT COURT'S RULING: Mandiant's report is not protected by the work product doctrine.

- Even though the threat of litigation was imminent when the Letter Agreement was signed, the court ruled that the report would have been prepared pursuant to the SOW even without the prospect of pending litigation.
- Because the SOW had dual purposes, both legal and business (and was originally designated only as business), the fact that the report was prepared at the direction of outside counsel was not dispositive.



Data Breach Class Actions: Substantive Issues

What can we learn from the *Capital One* ruling?

- 1) Have outside counsel retain the incident response consultant
- 2) Outside counsel should be *active* in the drafting of the incident report
- 3) If a report is needed for business purposes, prepare it separately, pursuant to a pre-existing SOW and out of “business” funds
- 4) Outside counsel must become the constructive “gatekeeper” of the report itself

For more detailed recommendations:

https://www.morrisonmahoney.com/writable/files/capital_one_client_alert.pdf



Safeguarding Data During the COVID-19 Pandemic

Communication

- Implement clear policies.
- Have easy-to-follow instructions to make and keep a home-working environment secure.
- Provide updates on suspicious links/emails, etc. as often as needed.

Execution

- Ensure that business owned (or managed) devices are kept secure.
- Every employee is now handling IT responsibilities
- Best practices need to extend to the home. Easier said than done.



Safeguarding Data During the COVID-19 Pandemic

Additional Considerations:

- How are users connecting to applications and video conferencing?
- Is there endpoint protection on ALL laptops and mobile devices?
- **Is multi-factor authentication being used?**
- Are exploits and malicious domains being blocked?
- Are Wi-fi networks being secured? Change default settings and passwords.
- Are employees keeping paper documents secure?
- **Are users reporting issues? VERY IMPORTANT!**



State of California Office of Administrative Law

In re:
Department of Justice

Regulatory Action:

Title 11, California Code of Regulations

APPROVED:

Adopt sections: 999.300, 999.301, 999.304,
999.305, 999.306, 999.307,
999.308, 999.312, 999.313,
999.314, 999.315, 999.316,
999.317, 999.318, 999.323,
999.324, 999.325, 999.326,
999.330, 999.331, 999.332,
999.336, 999.337

WITHDRAWN:

Adopt sections: 999.305(a)(5),
999.306(b)(2), 999.315(c),
999.326(c)

**AMENDED NOTICE OF APPROVAL IN PART
AND WITHDRAWAL IN PART OF
REGULATORY ACTION**

Government Code Section 11349.3

OAL Matter Number: 2020-0603-03

OAL Matter Type: Regular (S)

This action proposes new regulations to implement the California Consumer Privacy Act of 2018 (CCPA), which confers new privacy rights on consumers and imposes corresponding obligations on businesses subject to it.

OAL approves the sections listed as APPROVED above pursuant to section 11349.3 of the Government Code. This regulatory action becomes effective on 8/14/2020.

Proposed sections 999.305(a)(5), 999.306(b)(2), 999.315(c), and 999.326(c) listed as WITHDRAWN above, which required businesses to obtain express consent from consumers before using previously collected information for a materially different purpose, required businesses substantially interacting with consumers offline to provide notice of right to opt-out via an offline method, established minimum standards for submitting requests to opt-out to businesses, and provided businesses with the ability to deny certain requests from authorized agents, respectively, were withdrawn from OAL review pursuant to Government Code section 11349.3(c).

Please contact me at (916) 322-3761 or eric.partington@oal.ca.gov, or the OAL Reference Attorney at (916) 323-6815, if you have any questions about the resubmittal

process. You may request the return of your rulemaking record by contacting the OAL Front Desk at (916) 323-6225.

Date: August 27, 2020

A handwritten signature in black ink, appearing to read 'E. Partington', is written over a horizontal line.

Eric Partington
Senior Attorney

For: Kenneth J. Pogue
Director

Original: Xavier Becerra, Attorney
General

Copy: Julia Zuffelato

[2020 Cal AB 1281](#)

Chaptered, September 29, 2020

Reporter

2020 Cal ALS 268; 2020 Cal AB 1281; 2020 Cal Stats. ch. 268

CALIFORNIA ADVANCE LEGISLATIVE SERVICE > 2020 Regular Session > CHAPTER 268 > Assembly Bill No. 1281

Notice

Added: Text highlighted in green

Deleted: Red text with a strikethrough

Digest

LEGISLATIVE COUNSEL'S DIGEST

AB 1281, Chau. Privacy: **California Consumer Privacy Act** of 2018.

Existing law, the **California Consumer Privacy Act** of 2018, grants, commencing on January 1, 2020, a consumer various rights with regard to personal information relating to that consumer that is held by a business. The act, among other things, requires a business that collects personal information about a consumer to disclose the consumer's right to delete personal information in a form that is reasonably accessible to consumers and in accordance with a specified process. The act, until January 1, 2021, exempts from its provisions certain information collected by a business about a natural person in the course of the natural person acting as a job applicant, employee, owner, director, officer, medical staff member, or contractor, as specified. The act also, until January 1, 2021, exempts from specified provisions personal information reflecting a written or verbal communication or a transaction between the business and the consumer, if the consumer is a natural person who is acting as an employee, owner, director, officer, or contractor of a company, partnership, sole proprietorship, nonprofit, or government agency and whose communications or transaction with the business occur solely within the context of the business conducting due diligence regarding, or providing or receiving a product or service to or from that company, partnership, sole proprietorship, nonprofit, or government agency.

This bill would extend both exemptions until January 1, 2022.

This bill would specify that the operation of this extension is contingent upon voters not approving a specified ballot proposition at the November 3, 2020, statewide general election.

Synopsis

An act to amend *Section 1798.145 of the Civil Code*, relating to privacy.

[Approved by Governor September 29, 2020. Filed with Secretary of State September 29, 2020.]

Text

The people of the State of California do enact as follows:

SECTION 1. Section 1798.145 of the Civil Code is amended to read:

1798.145.

- (a) The obligations imposed on businesses by this title shall not restrict a business' ability to:
 - (1) Comply with federal, state, or local laws.
 - (2) Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, or local authorities.
 - (3) Cooperate with law enforcement agencies concerning conduct or activity that the business, service provider, or third party reasonably and in good faith believes may violate federal, state, or local law.
 - (4) Exercise or defend legal claims.
 - (5) Collect, use, retain, sell, or disclose consumer information that is deidentified or in the aggregate consumer information.
 - (6) Collect or sell a consumer's personal information if every aspect of that commercial conduct takes place wholly outside of California. For purposes of this title, commercial conduct takes place wholly outside of California if the business collected that information while the consumer was outside of California, no part of the sale of the consumer's personal information occurred in California, and no personal information collected while the consumer was in California is sold. This paragraph shall not permit a business from storing, including on a device, personal information about a consumer when the consumer is in California and then collecting that personal information when the consumer and stored personal information is outside of California.
- (b) The obligations imposed on businesses by Sections 1798.110 to 1798.135, inclusive, shall not apply where compliance by the business with the title would violate an evidentiary privilege under California law and shall not prevent a business from providing the personal information of a consumer to a person covered by an evidentiary privilege under California law as part of a privileged communication.
- (c)
 - (1) This title shall not apply to any of the following:
 - (A) Medical information governed by the Confidentiality of Medical Information Act (Part 2.6 (commencing with Section 56) of Division 1) or protected health information that is collected by a covered entity or business associate governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Accountability Act of 1996 (*Public Law 104-191*) and the Health Information Technology for Economic and Clinical Health Act (*Public Law 111-5*).
 - (B) A provider of health care governed by the Confidentiality of Medical Information Act (Part 2.6 (commencing with Section 56) of Division 1) or a covered entity governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Accountability Act of 1996 (*Public Law 104-191*), to the extent the provider or covered entity maintains patient information in the

2020 Cal AB 1281

same manner as medical information or protected health information as described in subparagraph (A) of this section.

(C) Information collected as part of a clinical trial subject to the Federal Policy for the Protection of Human Subjects, also known as the Common Rule, pursuant to good clinical practice guidelines issued by the International Council for Harmonisation or pursuant to human subject protection requirements of the United States Food and Drug Administration.

(2) For purposes of this subdivision, the definitions of “medical information” and “provider of health care” in Section 56.05 shall apply and the definitions of “business associate,” “covered entity,” and “protected health information” in [Section 160.103 of Title 45 of the Code of Federal Regulations](#) shall apply.

(d)

(1) This title shall not apply to an activity involving the collection, maintenance, disclosure, sale, communication, or use of any personal information bearing on a consumer’s credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living by a consumer reporting agency, as defined in subdivision (f) of Section 1681a of Title 15 of the United States Code, by a furnisher of information, as set forth in Section 1681s-2 of Title 15 of the United States Code, who provides information for use in a consumer report, as defined in subdivision (d) of Section 1681a of Title 15 of the United States Code, and by a user of a consumer report as set forth in Section 1681b of Title 15 of the United States Code.

(2) Paragraph (1) shall apply only to the extent that such activity involving the collection, maintenance, disclosure, sale, communication, or use of such information by that agency, furnisher, or user is subject to regulation under the Fair Credit Reporting Act, section 1681 et seq., Title 15 of the United States Code and the information is not used, communicated, disclosed, or sold except as authorized by the Fair Credit Reporting Act.

(3) This subdivision shall not apply to Section 1798.150.

(e) This title shall not apply to personal information collected, processed, sold, or disclosed pursuant to the federal Gramm-Leach-Bliley Act (*Public Law 106-102*), and implementing regulations, or the California Financial Information Privacy Act (Division 1.4 (commencing with [Section 4050 of the Financial Code](#))). This subdivision shall not apply to Section 1798.150.

(f) This title shall not apply to personal information collected, processed, sold, or disclosed pursuant to the Driver’s Privacy Protection Act of 1994 (18 U.S.C. Sec. 2721 et seq.). This subdivision shall not apply to Section 1798.150.

(g)

(1) Section 1798.120 shall not apply to vehicle information or ownership information retained or shared between a new motor vehicle dealer, as defined in [Section 426 of the Vehicle Code](#), and the vehicle’s manufacturer, as defined in [Section 672 of the Vehicle Code](#), if the vehicle or ownership information is shared for the purpose of effectuating, or in anticipation of effectuating, a vehicle repair covered by a vehicle warranty or a recall conducted pursuant to Sections 30118 to 30120, inclusive, of Title 49 of the United States Code, provided that the new motor vehicle dealer or vehicle manufacturer with which that vehicle information or ownership information is shared does not sell, share, or use that information for any other purpose.

(2) For purposes of this subdivision:

(A) “Vehicle information” means the vehicle information number, make, model, year, and odometer reading.

(B) “Ownership information” means the name or names of the registered owner or owners and the contact information for the owner or owners.

(h)

(1) This title shall not apply to any of the following:

- (A)** Personal information that is collected by a business about a natural person in the course of the natural person acting as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or contractor of that business to the extent that the natural person's personal information is collected and used by the business solely within the context of the natural person's role or former role as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or a contractor of that business.
- (B)** Personal information that is collected by a business that is emergency contact information of the natural person acting as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or contractor of that business to the extent that the personal information is collected and used solely within the context of having an emergency contact on file.
- (C)** Personal information that is necessary for the business to retain to administer benefits for another natural person relating to the natural person acting as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or contractor of that business to the extent that the personal information is collected and used solely within the context of administering those benefits.

(2) For purposes of this subdivision:

- (A)** "Contractor" means a natural person who provides any service to a business pursuant to a written contract.
- (B)** "Director" means a natural person designated in the articles of incorporation as such or elected by the incorporators and natural persons designated, elected, or appointed by any other name or title to act as directors, and their successors.
- (C)** "Medical staff member" means a licensed physician and surgeon, dentist, or podiatrist, licensed pursuant to Division 2 (commencing with [Section 500 of the Business and Professions Code](#) and a clinical psychologist as defined in [Section 1316.5 of the Health and Safety Code](#).
- (D)** "Officer" means a natural person elected or appointed by the board of directors to manage the daily operations of a corporation, such as a chief executive officer, president, secretary, or treasurer.
- (E)** "Owner" means a natural person who meets one of the following:
 - (i)** Has ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a business.
 - (ii)** Has control in any manner over the election of a majority of the directors or of individuals exercising similar functions.
 - (iii)** Has the power to exercise a controlling influence over the management of a company.

(3) This subdivision shall not apply to subdivision (b) of Section 1798.100 or Section 1798.150.**(4)** This subdivision shall become inoperative on January 1, ~~2021~~2022.**(i)** Notwithstanding a business' obligations to respond to and honor consumer rights requests pursuant to this title:

- (1)** A time period for a business to respond to any verified consumer request may be extended by up to 90 additional days where necessary, taking into account the complexity and number of the requests. The business shall inform the consumer of any such extension within 45 days of receipt of the request, together with the reasons for the delay.
- (2)** If the business does not take action on the request of the consumer, the business shall inform the consumer, without delay and at the latest within the time period permitted of response by this

section, of the reasons for not taking action and any rights the consumer may have to appeal the decision to the business.

- (3) If requests from a consumer are manifestly unfounded or excessive, in particular because of their repetitive character, a business may either charge a reasonable fee, taking into account the administrative costs of providing the information or communication or taking the action requested, or refuse to act on the request and notify the consumer of the reason for refusing the request. The business shall bear the burden of demonstrating that any verified consumer request is manifestly unfounded or excessive.
- (j) A business that discloses personal information to a service provider shall not be liable under this title if the service provider receiving the personal information uses it in violation of the restrictions set forth in the title, provided that, at the time of disclosing the personal information, the business does not have actual knowledge, or reason to believe, that the service provider intends to commit such a violation. A service provider shall likewise not be liable under this title for the obligations of a business for which it provides services as set forth in this title.
- (k) This title shall not be construed to require a business to collect personal information that it would not otherwise collect in the ordinary course of its business, retain personal information for longer than it would otherwise retain such information in the ordinary course of its business, or reidentify or otherwise link information that is not maintained in a manner that would be considered personal information.
- (l) The rights afforded to consumers and the obligations imposed on the business in this title shall not adversely affect the rights and freedoms of other consumers.
- (m) The rights afforded to consumers and the obligations imposed on any business under this title shall not apply to the extent that they infringe on the noncommercial activities of a person or entity described in subdivision (b) of [Section 2 of Article I of the California Constitution](#).
- (n)
- (1) The obligations imposed on businesses by Sections 1798.100, 1798.105, 1798.110, 1798.115, 1798.130, and 1798.135 shall not apply to personal information reflecting a written or verbal communication or a transaction between the business and the consumer, where the consumer is a natural person who is acting as an employee, owner, director, officer, or contractor of a company, partnership, sole proprietorship, ~~non-profit~~ nonprofit, or government agency and whose communications or transaction with the business occur solely within the context of the business conducting due diligence regarding, or providing or receiving a product or service to or from such company, partnership, sole proprietorship, ~~non-profit~~ nonprofit, or government agency.
- (2) For purposes of this subdivision:
- (A) "Contractor" means a natural person who provides any service to a business pursuant to a written contract.
- (B) "Director" means a natural person designated in the articles of incorporation as such or elected by the incorporators and natural persons designated, elected, or appointed by any other name or title to act as directors, and their successors.
- (C) "Officer" means a natural person elected or appointed by the board of directors to manage the daily operations of a corporation, such as a chief executive officer, president, secretary, or treasurer.
- (D) "Owner" means a natural person who meets one of the following:
- (i) Has ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a business.
- (ii) Has control in any manner over the election of a majority of the directors or of individuals exercising similar functions.

(iii) Has the power to exercise a controlling influence over the management of a company.

(3) This subdivision shall become inoperative on January 1, ~~2021~~2022.

SEC. 2.

This act shall become operative only if the voters do not approve any ballot proposition that amends *Section 1798.145 of the Civil Code* at the November 3, 2020, statewide general election.

History

Filed with Secretary of State September 29, 2020

Approved by the Governor September 29, 2020

Effective date: January 1, 2021

Sponsor

Chau

CALIFORNIA ADVANCE LEGISLATIVE SERVICE
Copyright © 2020 LexisNexis. All rights reserved.

End of Document

2020 Cal AB 713

Chaptered, September 25, 2020

Reporter

2020 Cal ALS 172; 2020 Cal AB 713; 2020 Cal Stats. ch. 172

CALIFORNIA ADVANCE LEGISLATIVE SERVICE > 2020 Regular Session > CHAPTER 172 > Assembly Bill No. 713

Notice

Added: Text highlighted in green

Digest

LEGISLATIVE COUNSEL'S DIGEST

AB 713, Mullin. **California Consumer Privacy Act** of 2018.

(1)

Existing law, the **California Consumer Privacy Act** of 2018 (CCPA), grants a consumer various rights with regard to personal information relating to that consumer collected by a business, including the right to know the categories and the specific pieces of personal information that have been collected and to opt out of the sale of personal information. The act also grants a consumer the right to request a business to delete any personal information about the consumer collected by the business and requires a business to do so upon receipt of a verified request, except as specified. The act excepts certain categories of personal information and entities from its provisions, including medical information, as specified.

This bill would except from the CCPA information that was deidentified in accordance with specified federal law, or was derived from medical information, protected health information, individually identifiable health information, or identifiable private information, consistent with specified federal policy, as provided. The bill also would except from the CCPA a business associate of a covered entity, as defined, that is governed by federal privacy, security, and data breach notification rules if the business associate maintains, uses, and discloses patient information in accordance with specified requirements. The bill would further except information that is collected for, used in, or disclosed in research, as defined. The bill would define terms for these purposes.

This bill would additionally prohibit a business or other person from reidentifying information that was deidentified, unless a specified exception is met. The bill would, beginning January 1, 2021, require a contract for the sale or license of deidentified information to include specified provisions relating to the prohibition of reidentification, as provided.

(2)

The CCPA requires a business to make certain disclosures to consumers, in a specified form, in its online privacy policy, if the business has an online privacy policy, and in any California-specific description of consumers' privacy

rights, or, if the business does not maintain an online privacy policy or policies, on its internet website, and to update that information at least once every 12 months.

This bill would require a business that sells or discloses information that was deidentified in accordance with specified federal law, was derived from protected health information, individually identifiable health information, or identifiable private information to also disclose whether the business sells or discloses deidentified patient information derived from patient information and, if so, whether that information was deidentified pursuant to specified methods.

(3)

This bill would declare that it is to take effect immediately as an urgency statute.

Synopsis

An act to amend Section 1798.130 of, and to add Sections 1798.146 and 1798.148 to, the Civil Code, relating to consumer privacy, and declaring the urgency thereof, to take effect immediately.

[Approved by Governor September 25, 2020. Filed with Secretary of State September 25, 2020.]

Text

The people of the State of California do enact as follows:

SECTION 1. Section [1798.130](#) of the Civil Code is amended to read:

1798.130.

(a) In order to comply with Sections 1798.100, 1798.105, 1798.110, 1798.115, and 1798.125, a business shall, in a form that is reasonably accessible to consumers:

(1)

(A) Make available to consumers two or more designated methods for submitting requests for information required to be disclosed pursuant to Sections 1798.110 and 1798.115, including, at a minimum, a toll-free telephone number. A business that operates exclusively online and has a direct relationship with a consumer from whom it collects personal information shall only be required to provide an email address for submitting requests for information required to be disclosed pursuant to Sections 1798.110 and 1798.115.

(B) If the business maintains an internet website, make the internet website available to consumers to submit requests for information required to be disclosed pursuant to Sections 1798.110 and 1798.115.

(2) Disclose and deliver the required information to a consumer free of charge within 45 days of receiving a verifiable consumer request from the consumer. The business shall promptly take steps to determine whether the request is a verifiable consumer request, but this shall not extend the business' duty to disclose and deliver the information within 45 days of receipt of the consumer's request. The time period to provide the required information may be extended once by an additional 45 days when reasonably necessary, provided the consumer is provided notice of the extension within the first 45-day period. The disclosure shall cover the 12-month period preceding the business' receipt of the verifiable consumer request and shall be made in writing and delivered through the consumer's account with the business, if the consumer maintains an account with the business, or by mail or electronically at the consumer's option if the consumer does not maintain

2020 Cal AB 713

an account with the business, in a readily useable format that allows the consumer to transmit this information from one entity to another entity without hindrance. The business may require authentication of the consumer that is reasonable in light of the nature of the personal information requested, but shall not require the consumer to create an account with the business in order to make a verifiable consumer request. If the consumer maintains an account with the business, the business may require the consumer to submit the request through that account.

(3) For purposes of subdivision (b) of Section 1798.110:

- (A)** To identify the consumer, associate the information provided by the consumer in the verifiable consumer request to any personal information previously collected by the business about the consumer.
- (B)** Identify by category or categories the personal information collected about the consumer in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describes the personal information collected.

(4) For purposes of subdivision (b) of Section 1798.115:

- (A)** Identify the consumer and associate the information provided by the consumer in the verifiable consumer request to any personal information previously collected by the business about the consumer.
- (B)** Identify by category or categories the personal information of the consumer that the business sold in the preceding 12 months by reference to the enumerated category in subdivision (c) that most closely describes the personal information, and provide the categories of third parties to whom the consumer's personal information was sold in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describes the personal information sold. The business shall disclose the information in a list that is separate from a list generated for the purposes of subparagraph (C).
- (C)** Identify by category or categories the personal information of the consumer that the business disclosed for a business purpose in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describes the personal information, and provide the categories of third parties to whom the consumer's personal information was disclosed for a business purpose in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describes the personal information disclosed. The business shall disclose the information in a list that is separate from a list generated for the purposes of subparagraph (B).

(5) Disclose the following information in its online privacy policy or policies if the business has an online privacy policy or policies and in any California-specific description of consumers' privacy rights, or if the business does not maintain those policies, on its internet website and update that information at least once every 12 months:

- (A)** A description of a consumer's rights pursuant to Sections 1798.100, 1798.105, 1798.110, 1798.115, and 1798.125 and one or more designated methods for submitting requests.
- (B)** For purposes of subdivision (c) of Section 1798.110, a list of the categories of personal information it has collected about consumers in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describe the personal information collected.
- (C)** For purposes of paragraphs (1) and (2) of subdivision (c) of Section 1798.115, two separate lists:
 - (i)** A list of the categories of personal information it has sold about consumers in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describe the personal information sold, or if the business has not sold

2020 Cal AB 713

consumers' personal information in the preceding 12 months, the business shall disclose that fact.

- (ii) A list of the categories of personal information it has disclosed about consumers for a business purpose in the preceding 12 months by reference to the enumerated category in subdivision (c) that most closely describe the personal information disclosed, or if the business has not disclosed consumers' personal information for a business purpose in the preceding 12 months, the business shall disclose that fact.

(D) In the case of a business that sells or discloses deidentified patient information not subject to this title pursuant to clause (i) of subparagraph (A) of paragraph (4) of subdivision (a) of Section 1798.146, whether the business sells or discloses deidentified patient information derived from patient information and if so, whether that patient information was deidentified pursuant to one or more of the following:

- (i) The deidentification methodology described in Section 164.514(b)(1) of Title 45 of the Code of Federal Regulations, commonly known as the HIPAA expert determination method.
- (ii) The deidentification methodology described in Section 164.514(b)(2) of Title 45 of the Code of Federal Regulations, commonly known as the HIPAA safe harbor method.

(6) Ensure that all individuals responsible for handling consumer inquiries about the business' privacy practices or the business' compliance with this title are informed of all requirements in Sections 1798.100, 1798.105, 1798.110, 1798.115, and 1798.125, and this section, and how to direct consumers to exercise their rights under those sections.

(7) Use any personal information collected from the consumer in connection with the business' verification of the consumer's request solely for the purposes of verification.

(b) A business is not obligated to provide the information required by Sections 1798.110 and 1798.115 to the same consumer more than twice in a 12-month period.

(c) The categories of personal information required to be disclosed pursuant to Sections 1798.110 and 1798.115 shall follow the definition of personal information in Section 1798.140.

SEC. 2. Section [1798.146](#) is added to the Civil Code, to read:

1798.146.

(a) This title shall not apply to any of the following:

- (1)** Medical information governed by the Confidentiality of Medical Information Act (Part 2.6 (commencing with Section 56) of Division 1) or protected health information that is collected by a covered entity or business associate governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the federal Health Insurance Portability and Accountability Act of 1996 (*Public Law 104-191*) and the federal Health Information Technology for Economic and Clinical Health Act, Title XIII of the federal American Recovery and Reinvestment Act of 2009 (*Public Law 111-5*).
- (2)** A provider of health care governed by the Confidentiality of Medical Information Act (Part 2.6 (commencing with Section 56) of Division 1) or a covered entity governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the federal Health Insurance Portability and Accountability Act of 1996 (*Public Law 104-191*), to the extent the provider or covered entity maintains, uses, and discloses patient information in the same manner as medical information or protected health information as described in paragraph (1).

(3) A business associate of a covered entity governed by the privacy, security, and data breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the federal Health Insurance Portability and Accountability Act of 1996 (*Public Law 104-191*) and the federal Health Information Technology for Economic and Clinical Health Act, Title XIII of the federal American Recovery and Reinvestment Act of 2009 (*Public Law 111-5*), to the extent that the business associate maintains, uses, and discloses patient information in the same manner as medical information or protected health information as described in paragraph (1).

(4)

(A) Information that meets both of the following conditions:

(i) It is deidentified in accordance with the requirements for deidentification set forth in Section 164.514 of Part 164 of Title 45 of the Code of Federal Regulations.

(ii) It is derived from patient information that was originally collected, created, transmitted, or maintained by an entity regulated by the Health Insurance Portability and Accountability Act, the Confidentiality Of Medical Information Act, or the Federal Policy for the Protection of Human Subjects, also known as the Common Rule.

(B) Information that met the requirements of subparagraph (A) but is subsequently reidentified shall no longer be eligible for the exemption in this paragraph, and shall be subject to applicable federal and state data privacy and security laws, including, but not limited to, the Health Insurance Portability and Accountability Act, the Confidentiality Of Medical Information Act, and this title.

(5) Information that is collected, used, or disclosed in research, as defined in Section 164.501 of Title 45 of the Code of Federal Regulations, including, but not limited to, a clinical trial, and that is conducted in accordance with applicable ethics, confidentiality, privacy, and security rules of Part 164 of Title 45 of the Code of Federal Regulations, the Federal Policy for the Protection of Human Subjects, also known as the Common Rule, good clinical practice guidelines issued by the International Council for Harmonisation, or human subject protection requirements of the United States Food and Drug Administration.

(b) For purposes of this section, all of the following shall apply:

(1) "Business associate" has the same meaning as defined in Section 160.103 of Title 45 of the Code of Federal Regulations.

(2) "Covered entity" has the same meaning as defined in Section 160.103 of Title 45 of the Code of Federal Regulations.

(3) "Identifiable private information" has the same meaning as defined in Section 46.102 of Title 45 of the Code of Federal Regulations.

(4) "Individually identifiable health information" has the same meaning as defined in Section 160.103 of Title 45 of the Code of Federal Regulations.

(5) "Medical information" has the same meaning as defined in Section 56.05.

(6) "Patient information" shall mean identifiable private information, protected health information, individually identifiable health information, or medical information.

(7) "Protected health information" has the same meaning as defined in Section 160.103 of Title 45 of the Code of Federal Regulations.

(8) "Provider of health care" has the same meaning as defined in Section 56.05.

SEC. 3. Section [1798.148](#) is added to the Civil Code, to read:

1798.148.

- (a) A business or other person shall not reidentify, or attempt to reidentify, information that has met the requirements of paragraph (4) of subdivision (a) of Section 1798.146, except for one or more of the following purposes:
- (1) Treatment, payment, or health care operations conducted by a covered entity or business associate acting on behalf of, and at the written direction of, the covered entity. For purposes of this paragraph, "treatment," "payment," "health care operations," "covered entity," and "business associate" have the same meaning as defined in Section 164.501 of Title 45 of the Code of Federal Regulations.
 - (2) Public health activities or purposes as described in Section 164.512 of Title 45 of the Code of Federal Regulations.
 - (3) Research, as defined in Section 164.501 of Title 45 of the Code of Federal Regulations, that is conducted in accordance with Part 46 of Title 45 of the Code of Federal Regulations, the Federal Policy for the Protection of Human Subjects, also known as the Common Rule.
 - (4) Pursuant to a contract where the lawful holder of the deidentified information that met the requirements of paragraph (4) of subdivision (a) of Section 1798.146 expressly engages a person or entity to attempt to reidentify the deidentified information in order to conduct testing, analysis, or validation of deidentification, or related statistical techniques, if the contract bans any other use or disclosure of the reidentified information and requires the return or destruction of the information that was reidentified upon completion of the contract.
 - (5) If otherwise required by law.
- (b) In accordance with paragraph (4) of subdivision (a) of Section 1798.146, information reidentified pursuant this section shall be subject to applicable federal and state data privacy and security laws including, but not limited to, the Health Insurance Portability and Accountability Act, the Confidentiality of Medical Information Act, and this title.
- (c) Beginning January 1, 2021, any contract for the sale or license of deidentified information that has met the requirements of paragraph (4) of subdivision (a) of Section 1798.146, where one of the parties is a person residing or doing business in the state, shall include the following, or substantially similar, provisions:
- (1) A statement that the deidentified information being sold or licensed includes deidentified patient information.
 - (2) A statement that reidentification, and attempted reidentification, of the deidentified information by the purchaser or licensee of the information is prohibited pursuant to this section.
 - (3) A requirement that, unless otherwise required by law, the purchaser or licensee of the deidentified information may not further disclose the deidentified information to any third party unless the third party is contractually bound by the same or stricter restrictions and conditions.
- (d) For purposes of this section, "reidentify" means the process of reversal of deidentification techniques, including, but not limited to, the addition of specific pieces of information or data elements that can, individually or in combination, be used to uniquely identify an individual or usage of any statistical method, contrivance, computer software, or other means that have the effect of associating deidentified information with a specific identifiable individual.

SEC. 4.

This act is an urgency statute necessary for the immediate preservation of the public peace, health, or safety within the meaning of Article IV of the California Constitution and shall go into immediate effect. The facts constituting the necessity are:

2020 Cal AB 713

The **California Consumer Privacy Act** of 2018 became operative on January 1, 2020, and will negatively impact certain health-related information and research. The provisions of this act would mitigate that harm as soon as possible by preserving access to information needed to conduct important health-related research that will benefit Californians.

History

Filed with Secretary of State September 25, 2020

Approved by the Governor September 25, 2020

Effective date: September 25, 2020

Sponsor

Mullin

CALIFORNIA ADVANCE LEGISLATIVE SERVICE
Copyright © 2020 LexisNexis. All rights reserved.

End of Document

FINAL TEXT OF PROPOSED REGULATIONS

TITLE 11. LAW

DIVISION 1. ATTORNEY GENERAL

CHAPTER 20. CALIFORNIA CONSUMER PRIVACY ACT REGULATIONS

Article 1. GENERAL PROVISIONS

§ 999.300. Title and Scope.

- (a) This Chapter shall be known as the California Consumer Privacy Act Regulations. It may be cited as such and will be referred to in this Chapter as “these regulations.” These regulations govern compliance with the California Consumer Privacy Act and do not limit any other rights that consumers may have.
- (b) A violation of these regulations shall constitute a violation of the CCPA and be subject to the remedies provided for therein.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.110, 1798.115, 1798.120, 1798.125, 1798.130, 1798.135, 1798.140, 1798.145, 1798.150, 1798.155 and 1798.185, Civil Code.

§ 999.301. Definitions.

In addition to the definitions set forth in Civil Code section 1798.140, for purposes of these regulations:

- (a) “Affirmative authorization” means an action that demonstrates the intentional decision by the consumer to opt-in to the sale of personal information. Within the context of a parent or guardian acting on behalf of a consumer under 13 years of age, it means that the parent or guardian has provided consent to the sale of the consumer’s personal information in accordance with the methods set forth in section 999.330. For consumers 13 years of age and older, it is demonstrated through a two-step process whereby the consumer shall first, clearly request to opt-in and then second, separately confirm their choice to opt-in.
- (b) “Attorney General” means the California Attorney General or any officer or employee of the California Department of Justice acting under the authority of the California Attorney General.
- (c) “Authorized agent” means a natural person or a business entity registered with the Secretary of State to conduct business in California that a consumer has authorized to act on their behalf subject to the requirements set forth in section 999.326.
- (d) “Categories of sources” means types or groupings of persons or entities from which a business collects personal information about consumers, described with enough particularity to provide consumers with a meaningful understanding of the type of person or entity. They

may include the consumer directly, advertising networks, internet service providers, data analytics providers, government entities, operating systems and platforms, social networks, and data brokers.

- (e) “Categories of third parties” means types or groupings of third parties with whom the business shares personal information, described with enough particularity to provide consumers with a meaningful understanding of the type of third party. They may include advertising networks, internet service providers, data analytics providers, government entities, operating systems and platforms, social networks, and data brokers.
- (f) “CCPA” means the California Consumer Privacy Act of 2018, Civil Code sections 1798.100 *et seq.*
- (g) “COPPA” means the Children’s Online Privacy Protection Act, 15 U.S.C. sections 6501 to 6508 and 16 Code of Federal Regulations part 312.5.
- (h) “Employment benefits” means retirement, health, and other benefit programs, services, or products to which consumers and their dependents or their beneficiaries receive access through the consumer’s employer.
- (i) “Employment-related information” means personal information that is collected by the business about a natural person for the reasons identified in Civil Code section 1798.145, subdivision (h)(1). The collection of employment-related information, including for the purpose of administering employment benefits, shall be considered a business purpose.
- (j) “Financial incentive” means a program, benefit, or other offering, including payments to consumers, related to the collection, deletion, or sale of personal information.
- (k) “Household” means a person or group of people who: (1) reside at the same address, (2) share a common device or the same service provided by a business, and (3) are identified by the business as sharing the same group account or unique identifier.
- (l) “Notice at collection” means the notice given by a business to a consumer at or before the point at which a business collects personal information from the consumer as required by Civil Code section 1798.100, subdivision (b), and specified in these regulations.
- (m) “Notice of right to opt-out” means the notice given by a business informing consumers of their right to opt-out of the sale of their personal information as required by Civil Code sections 1798.120 and 1798.135 and specified in these regulations.
- (n) “Notice of financial incentive” means the notice given by a business explaining each financial incentive or price or service difference as required by Civil Code section 1798.125, subdivision (b), and specified in these regulations.
- (o) “Price or service difference” means (1) any difference in the price or rate charged for any goods or services to any consumer related to the collection, retention, or sale of personal information, including through the use of discounts, financial payments, or other benefits or penalties; or (2) any difference in the level or quality of any goods or services offered to any consumer related to the collection, retention, or sale of personal information, including the denial of goods or services to the consumer.

- (p) “Privacy policy,” as referred to in Civil Code section 1798.130, subdivision (a)(5), means the statement that a business shall make available to consumers describing the business’s practices, both online and offline, regarding the collection, use, disclosure, and sale of personal information, and of the rights of consumers regarding their own personal information.
- (q) “Request to delete” means a consumer request that a business delete personal information about the consumer that the business has collected from the consumer, pursuant to Civil Code section 1798.105.
- (r) “Request to know” means a consumer request that a business disclose personal information that it has collected about the consumer pursuant to Civil Code sections 1798.100, 1798.110, or 1798.115. It includes a request for any or all of the following:
- (1) Specific pieces of personal information that a business has collected about the consumer;
 - (2) Categories of personal information it has collected about the consumer;
 - (3) Categories of sources from which the personal information is collected;
 - (4) Categories of personal information that the business sold or disclosed for a business purpose about the consumer;
 - (5) Categories of third parties to whom the personal information was sold or disclosed for a business purpose; and
 - (6) The business or commercial purpose for collecting or selling personal information.
- (s) “Request to opt-in” means the affirmative authorization that the business may sell personal information about the consumer by a parent or guardian of a consumer less than 13 years of age, by a consumer at least 13 and less than 16 years of age, or by a consumer who had previously opted out of the sale of their personal information.
- (t) “Request to opt-out” means a consumer request that a business not sell the consumer’s personal information to third parties, pursuant to Civil Code section 1798.120, subdivision (a).
- (u) “Signed” means that the written attestation, declaration, or permission has either been physically signed or provided electronically in accordance with the Uniform Electronic Transactions Act, Civil Code section 1633.1 et seq.
- (v) “Third-party identity verification service” means a security process offered by an independent third party that verifies the identity of the consumer making a request to the business. Third-party identity verification services are subject to the requirements set forth in Article 4 regarding requests to know and requests to delete.
- (w) “Value of the consumer’s data” means the value provided to the business by the consumer’s data as calculated under section 999.337.

- (x) “Verify” means to determine that the consumer making a request to know or request to delete is the consumer about whom the business has collected information, or if that consumer is less than 13 years of age, the consumer’s parent or legal guardian.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.110, 1798.115, 1798.120, 1798.125, 1798.130, 1798.135, 1798.140, 1798.145 and 1798.185, Civil Code.

Article 2. NOTICES TO CONSUMERS

§ 999.304. Overview of Required Notices.

- (a) Every business that must comply with the CCPA and these regulations shall provide a privacy policy in accordance with the CCPA and section 999.308.
- (b) A business that collects personal information from a consumer shall provide a notice at collection in accordance with the CCPA and section 999.305.
- (c) A business that sells personal information shall provide a notice of right to opt-out in accordance with the CCPA and section 999.306.
- (d) A business that offers a financial incentive or price or service difference shall provide a notice of financial incentive in accordance with the CCPA and section 999.307.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.115, 1798.120, 1798.125, 1798.130 and 1798.135, Civil Code.

§ 999.305. Notice at Collection of Personal Information.

(a) Purpose and General Principles

- (1) The purpose of the notice at collection is to provide consumers with timely notice, at or before the point of collection, about the categories of personal information to be collected from them and the purposes for which the personal information will be used.
- (2) The notice at collection shall be designed and presented in a way that is easy to read and understandable to consumers. The notice shall:
- a. Use plain, straightforward language and avoid technical or legal jargon.
 - b. Use a format that draws the consumer’s attention to the notice and makes the notice readable, including on smaller screens, if applicable.
 - c. Be available in the languages in which the business in its ordinary course provides contracts, disclaimers, sale announcements, and other information to consumers in California.
 - d. Be reasonably accessible to consumers with disabilities. For notices provided online, the business shall follow generally recognized industry standards, such as the Web Content Accessibility Guidelines, version 2.1 of June 5, 2018, from the World Wide Web Consortium, incorporated herein by reference. In other

contexts, the business shall provide information on how a consumer with a disability may access the notice in an alternative format.

(3) The notice at collection shall be made readily available where consumers will encounter it at or before the point of collection of any personal information.

Illustrative examples follow:

- a. When a business collects consumers' personal information online, it may post a conspicuous link to the notice on the introductory page of the business's website and on all webpages where personal information is collected.
 - b. When a business collects personal information through a mobile application, it may provide a link to the notice on the mobile application's download page and within the application, such as through the application's settings menu.
 - c. When a business collects consumers' personal information offline, it may include the notice on printed forms that collect personal information, provide the consumer with a paper version of the notice, or post prominent signage directing consumers to where the notice can be found online.
 - d. When a business collects personal information over the telephone or in person, it may provide the notice orally.
- (4) When a business collects personal information from a consumer's mobile device for a purpose that the consumer would not reasonably expect, it shall provide a just-in-time notice containing a summary of the categories of personal information being collected and a link to the full notice at collection. For example, if the business offers a flashlight application and the application collects geolocation information, the business shall provide a just-in-time notice, such as through a pop-up window when the consumer opens the application, that contains the information required by this subsection.
- (5) A business shall not collect categories of personal information other than those disclosed in the notice at collection. If the business intends to collect additional categories of personal information, the business shall provide a new notice at collection.
- (6) If a business does not give the notice at collection to the consumer at or before the point of collection of their personal information, the business shall not collect personal information from the consumer.

(b) A business shall include the following in its notice at collection:

- (1) A list of the categories of personal information about consumers to be collected. Each category of personal information shall be written in a manner that provides consumers a meaningful understanding of the information being collected.
- (2) The business or commercial purpose(s) for which the categories of personal information will be used.

- (3) If the business sells personal information, the link titled “Do Not Sell My Personal Information” required by section 999.315, subsection (a), or in the case of offline notices, where the webpage can be found online.
 - (4) A link to the business’s privacy policy, or in the case of offline notices, where the privacy policy can be found online.
- (c) If a business collects personal information from a consumer online, the notice at collection may be given to the consumer by providing a link to the section of the business’s privacy policy that contains the information required in subsection (b).
- (d) A business that does not collect personal information directly from the consumer does not need to provide a notice at collection to the consumer if it does not sell the consumer’s personal information.
- (e) A data broker registered with the Attorney General pursuant to Civil Code section 1798.99.80 *et seq.* does not need to provide a notice at collection to the consumer if it has included in its registration submission a link to its online privacy policy that includes instructions on how a consumer can submit a request to opt-out.
- (f) A business collecting employment-related information shall comply with the provisions of section 999.305 except with regard to the following:
 - (1) The notice at collection of employment-related information does not need to include the link or web address to the link titled “Do Not Sell My Personal Information”.
 - (2) The notice at collection of employment-related information is not required to provide a link to the business’s privacy policy.
- (g) Subsection (f) shall become inoperative on January 1, 2021, unless the CCPA is amended otherwise.

Note: Authority: Section 1798.185, Civil Code. Reference: Sections 1798.99.82, 1798.100, 1798.115 and 1798.185, Civil Code.

§ 999.306. Notice of Right to Opt-Out of Sale of Personal Information.

(a) Purpose and General Principles

- (1) The purpose of the notice of right to opt-out is to inform consumers of their right to direct a business that sells their personal information to stop selling their personal information.
- (2) The notice of right to opt-out shall be designed and presented in a way that is easy to read and understandable to consumers. The notice shall:
 - a. Use plain, straightforward language and avoid technical or legal jargon.
 - b. Use a format that draws the consumer’s attention to the notice and makes the notice readable, including on smaller screens, if applicable.

- c. Be available in the languages in which the business in its ordinary course provides contracts, disclaimers, sale announcements, and other information to consumers in California.
 - d. Be reasonably accessible to consumers with disabilities. For notices provided online, the business shall follow generally recognized industry standards, such as the Web Content Accessibility Guidelines, version 2.1 of June 5, 2018, from the World Wide Web Consortium, incorporated herein by reference. In other contexts, the business shall provide information on how a consumer with a disability may access the notice in an alternative format.
- (b) A business that sells the personal information of consumers shall provide the notice of right to opt-out to consumers as follows:
 - (1) A business shall post the notice of right to opt-out on the Internet webpage to which the consumer is directed after clicking on the “Do Not Sell My Personal Information” link on the website homepage or the download or landing page of a mobile application. In addition, a business that collects personal information through a mobile application may provide a link to the notice within the application, such as through the application’s settings menu. The notice shall include the information specified in subsection (c) or link to the section of the business’s privacy policy that contains the same information.
 - (2) A business that does not operate a website shall establish, document, and comply with another method by which it informs consumers of their right to opt-out. That method shall comply with the requirements set forth in subsection (a)(2).
- (c) A business shall include the following in its notice of right to opt-out:
 - (1) A description of the consumer’s right to opt-out of the sale of their personal information by the business;
 - (2) The interactive form by which the consumer can submit their request to opt-out online, as required by section 999.315, subsection (a), or if the business does not operate a website, the offline method by which the consumer can submit their request to opt-out; and
 - (3) Instructions for any other method by which the consumer may submit their request to opt-out.
- (d) A business does not need to provide a notice of right to opt-out if:
 - (1) It does not sell personal information; and
 - (2) It states in its privacy policy that it does not sell personal information.
- (e) A business shall not sell the personal information it collected during the time the business did not have a notice of right to opt-out posted unless it obtains the affirmative authorization of the consumer.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.120, 1798.135 and 1798.185, Civil Code.

§ 999.307. Notice of Financial Incentive.

(a) Purpose and General Principles

- (1) The purpose of the notice of financial incentive is to explain to the consumer the material terms of a financial incentive or price or service difference the business is offering so that the consumer may make an informed decision about whether to participate. A business that does not offer a financial incentive or price or service difference is not required to provide a notice of financial incentive.
- (2) The notice of financial incentive shall be designed and presented in a way that is easy to read and understandable to consumers. The notice shall:
 - a. Use plain, straightforward language and avoid technical or legal jargon.
 - b. Use a format that draws the consumer's attention to the notice and makes the notice readable, including on smaller screens, if applicable.
 - c. Be available in the languages in which the business in its ordinary course provides contracts, disclaimers, sale announcements, and other information to consumers in California.
 - d. Be reasonably accessible to consumers with disabilities. For notices provided online, the business shall follow generally recognized industry standards, such as the Web Content Accessibility Guidelines, version 2.1 of June 5, 2018, from the World Wide Web Consortium, incorporated herein by reference. In other contexts, the business shall provide information on how a consumer with a disability may access the notice in an alternative format.
 - e. Be readily available where consumers will encounter it before opting-in to the financial incentive or price or service difference.
- (3) If the business offers the financial incentive or price or service difference online, the notice may be given by providing a link to the section of a business's privacy policy that contains the information required in subsection (b).

(b) A business shall include the following in its notice of financial incentive:

- (1) A succinct summary of the financial incentive or price or service difference offered;
- (2) A description of the material terms of the financial incentive or price or service difference, including the categories of personal information that are implicated by the financial incentive or price or service difference and the value of the consumer's data;
- (3) How the consumer can opt-in to the financial incentive or price or service difference;
- (4) A statement of the consumer's right to withdraw from the financial incentive at any time and how the consumer may exercise that right; and
- (5) An explanation of how the financial incentive or price or service difference is reasonably related to the value of the consumer's data, including:

- a. A good-faith estimate of the value of the consumer's data that forms the basis for offering the financial incentive or price or service difference; and
- b. A description of the method the business used to calculate the value of the consumer's data.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.125 and 1798.130, Civil Code.

§ 999.308. Privacy Policy.

(a) Purpose and General Principles

- (1) The purpose of the privacy policy is to provide consumers with a comprehensive description of a business's online and offline practices regarding the collection, use, disclosure, and sale of personal information and of the rights of consumers regarding their personal information.
- (2) The privacy policy shall be designed and presented in a way that is easy to read and understandable to consumers. The policy shall:
 - a. Use plain, straightforward language and avoid technical or legal jargon.
 - b. Use a format that makes the policy readable, including on smaller screens, if applicable.
 - c. Be available in the languages in which the business in its ordinary course provides contracts, disclaimers, sale announcements, and other information to consumers in California.
 - d. Be reasonably accessible to consumers with disabilities. For notices provided online, the business shall follow generally recognized industry standards, such as the Web Content Accessibility Guidelines, version 2.1 of June 5, 2018, from the World Wide Web Consortium, incorporated herein by reference. In other contexts, the business shall provide information on how a consumer with a disability may access the policy in an alternative format.
 - e. Be available in a format that allows a consumer to print it out as a document.
- (b) The privacy policy shall be posted online through a conspicuous link using the word "privacy" on the business's website homepage or on the download or landing page of a mobile application. If the business has a California-specific description of consumers' privacy rights on its website, then the privacy policy shall be included in that description. A business that does not operate a website shall make the privacy policy conspicuously available to consumers. A mobile application may include a link to the privacy policy in the application's settings menu.
- (c) The privacy policy shall include the following information:
 - (1) Right to Know About Personal Information Collected, Disclosed, or Sold.

- a. Explanation that a consumer has the right to request that the business disclose what personal information it collects, uses, discloses, and sells.
- b. Instructions for submitting a verifiable consumer request to know and links to an online request form or portal for making the request, if offered by the business.
- c. General description of the process the business will use to verify the consumer request, including any information the consumer must provide.
- d. Identification of the categories of personal information the business has collected about consumers in the preceding 12 months. The categories shall be described in a manner that provides consumers a meaningful understanding of the information being collected.
- e. Identification of the categories of sources from which the personal information is collected.
- f. Identification of the business or commercial purpose for collecting or selling personal information. The purpose shall be described in a manner that provides consumers a meaningful understanding of why the information is collected or sold.
- g. Disclosure or Sale of Personal Information.
 - 1. Identification of the categories of personal information, if any, that the business has disclosed for a business purpose or sold to third parties in the preceding 12 months.
 - 2. For each category of personal information identified, the categories of third parties to whom the information was disclosed or sold.
 - 3. Statement regarding whether the business has actual knowledge that it sells the personal information of consumers under 16 years of age.

(2) Right to Request Deletion of Personal Information.

- a. Explanation that the consumer has a right to request the deletion of their personal information collected by the business.
- b. Instructions for submitting a verifiable consumer request to delete and links to an online request form or portal for making the request, if offered by the business.
- c. General description of the process the business will use to verify the consumer request, including any information the consumer must provide.

(3) Right to Opt-Out of the Sale of Personal Information.

- a. Explanation that the consumer has a right to opt-out of the sale of their personal information by a business.
- b. Statement regarding whether or not the business sells personal information. If the business sells personal information, include either the contents of the notice of right to opt-out or a link to it in accordance with section 999.306.

- (4) Right to Non-Discrimination for the Exercise of a Consumer's Privacy Rights.
 - a. Explanation that the consumer has a right not to receive discriminatory treatment by the business for the exercise of the privacy rights conferred by the CCPA.
- (5) Authorized Agent.
 - a. Instructions on how an authorized agent can make a request under the CCPA on the consumer's behalf.
- (6) Contact for More Information.
 - a. A contact for questions or concerns about the business's privacy policies and practices using a method reflecting the manner in which the business primarily interacts with the consumer.
- (7) Date the privacy policy was last updated.
- (8) If subject to the requirements set forth in section 999.317, subsection (g), the information compiled in section 999.317, subsection (g)(1), or a link to it.
- (9) If the business has actual knowledge that it sells the personal information of consumers under 16 years of age, a description of the processes required by sections 999.330 and 999.331.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.105, 1798.115, 1798.120, 1798.125 and 1798.130, Civil Code.

Article 3. BUSINESS PRACTICES FOR HANDLING CONSUMER REQUESTS

§ 999.312. Methods for Submitting Requests to Know and Requests to Delete.

- (a) A business that operates exclusively online and has a direct relationship with a consumer from whom it collects personal information shall only be required to provide an email address for submitting requests to know. All other businesses shall provide two or more designated methods for submitting requests to know, including, at a minimum, a toll-free telephone number. Other acceptable methods for submitting these requests include, but are not limited to, a designated email address, a form submitted in person, and a form submitted through the mail.
- (b) A business shall provide two or more designated methods for submitting requests to delete. Acceptable methods for submitting these requests include, but are not limited to, a toll-free phone number, a link or form available online through a business's website, a designated email address, a form submitted in person, and a form submitted through the mail.
- (c) A business shall consider the methods by which it primarily interacts with consumers when determining which methods to provide for submitting requests to know and requests to delete. If the business interacts with consumers in person, the business shall consider providing an in-person method such as a printed form the consumer can directly submit or send by mail, a tablet or computer portal that allows the consumer to complete and submit

an online form, or a telephone with which the consumer can call the business's toll-free number.

- (d) A business may use a two-step process for online requests to delete where the consumer must first, submit the request to delete and then second, separately confirm that they want their personal information deleted.
- (e) If a consumer submits a request in a manner that is not one of the designated methods of submission, or is deficient in some manner unrelated to the verification process, the business shall either:
 - (1) Treat the request as if it had been submitted in accordance with the business's designated manner, or
 - (2) Provide the consumer with information on how to submit the request or remedy any deficiencies with the request, if applicable.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.110, 1798.115, 1798.130, 1798.140 and 1798.185, Civil Code.

§ 999.313. Responding to Requests to Know and Requests to Delete.

- (a) Upon receiving a request to know or a request to delete, a business shall confirm receipt of the request within 10 business days and provide information about how the business will process the request. The information provided shall describe in general the business's verification process and when the consumer should expect a response, except in instances where the business has already granted or denied the request. The confirmation may be given in the same manner in which the request was received. For example, if the request is made over the phone, the confirmation may be given orally during the phone call.
- (b) Businesses shall respond to requests to know and requests to delete within 45 calendar days. The 45-day period will begin on the day that the business receives the request, regardless of time required to verify the request. If the business cannot verify the consumer within the 45-day time period, the business may deny the request. If necessary, businesses may take up to an additional 45 calendar days to respond to the consumer's request, for a maximum total of 90 calendar days from the day the request is received, provided that the business provides the consumer with notice and an explanation of the reason that the business will take more than 45 days to respond to the request.
- (c) Responding to Requests to Know.
 - (1) For requests that seek the disclosure of specific pieces of information about the consumer, if a business cannot verify the identity of the person making the request pursuant to the regulations set forth in Article 4, the business shall not disclose any specific pieces of personal information to the requestor and shall inform the requestor that it cannot verify their identity. If the request is denied in whole or in part, the business shall also evaluate the consumer's request as if it is seeking the disclosure of categories of personal information about the consumer pursuant to subsection (c)(2).

- (2) For requests that seek the disclosure of categories of personal information about the consumer, if a business cannot verify the identity of the person making the request pursuant to the regulations set forth in Article 4, the business may deny the request to disclose the categories and other information requested and shall inform the requestor that it cannot verify their identity. If the request is denied in whole or in part, the business shall provide or direct the consumer to its general business practices regarding the collection, maintenance, and sale of personal information set forth in its privacy policy.
- (3) In responding to a request to know, a business is not required to search for personal information if all of the following conditions are met:
- a. The business does not maintain the personal information in a searchable or reasonably accessible format;
 - b. The business maintains the personal information solely for legal or compliance purposes;
 - c. The business does not sell the personal information and does not use it for any commercial purpose; and
 - d. The business describes to the consumer the categories of records that may contain personal information that it did not search because it meets the conditions stated above.
- (4) A business shall not disclose in response to a request to know a consumer's Social Security number, driver's license number or other government-issued identification number, financial account number, any health insurance or medical identification number, an account password, security questions and answers, or unique biometric data generated from measurements or technical analysis of human characteristics. The business shall, however, inform the consumer with sufficient particularity that it has collected the type of information. For example, a business shall respond that it collects "unique biometric data including a fingerprint scan" without disclosing the actual fingerprint scan data.
- (5) If a business denies a consumer's verified request to know specific pieces of personal information, in whole or in part, because of a conflict with federal or state law, or an exception to the CCPA, the business shall inform the requestor and explain the basis for the denial, unless prohibited from doing so by law. If the request is denied only in part, the business shall disclose the other information sought by the consumer.
- (6) A business shall use reasonable security measures when transmitting personal information to the consumer.
- (7) If a business maintains a password-protected account with the consumer, it may comply with a request to know by using a secure self-service portal for consumers to access, view, and receive a portable copy of their personal information if the portal

fully discloses the personal information that the consumer is entitled to under the CCPA and these regulations, uses reasonable data security controls, and complies with the verification requirements set forth in Article 4.

(8) Unless otherwise specified by the business to cover a longer period of time, the 12-month period covered by a consumer's verifiable request to know referenced in Civil Code section 1798.130, subdivision (a)(2), shall run from the date the business receives the request, regardless of the time required to verify the request.

(9) In responding to a consumer's verified request to know categories of personal information, categories of sources, and/or categories of third parties, a business shall provide an individualized response to the consumer as required by the CCPA. It shall not refer the consumer to the businesses' general practices outlined in its privacy policy unless its response would be the same for all consumers and the privacy policy discloses all the information that is otherwise required to be in a response to a request to know such categories.

(10) In responding to a verified request to know categories of personal information, the business shall provide:

- a. The categories of personal information the business has collected about the consumer in the preceding 12 months;
- b. The categories of sources from which the personal information was collected;
- c. The business or commercial purpose for which it collected or sold the personal information;
- d. The categories of third parties with whom the business shares personal information;
- e. The categories of personal information that the business sold in the preceding 12 months, and for each category identified, the categories of third parties to whom it sold that particular category of personal information; and
- f. The categories of personal information that the business disclosed for a business purpose in the preceding 12 months, and for each category identified, the categories of third parties to whom it disclosed that particular category of personal information.

(11) A business shall identify the categories of personal information, categories of sources of personal information, and categories of third parties to whom a business sold or disclosed personal information, in a manner that provides consumers a meaningful understanding of the categories listed.

(d) Responding to Requests to Delete.

- (1) For requests to delete, if a business cannot verify the identity of the requestor pursuant to the regulations set forth in Article 4, the business may deny the request to delete. The business shall inform the requestor that their identity cannot be verified.
- (2) A business shall comply with a consumer's request to delete their personal information by:

 - a. Permanently and completely erasing the personal information on its existing systems with the exception of archived or back-up systems;
 - b. Deidentifying the personal information; or
 - c. Aggregating the consumer information.
- (3) If a business stores any personal information on archived or backup systems, it may delay compliance with the consumer's request to delete, with respect to data stored on the archived or backup system, until the archived or backup system relating to that data is restored to an active system or next accessed or used for a sale, disclosure, or commercial purpose.
- (4) In responding to a request to delete, a business shall inform the consumer whether or not it has complied with the consumer's request.
- (5) If the business complies with the consumer's request, the business shall inform the consumer that it will maintain a record of the request as required by section 999.317, subsection (b). A business may retain a record of the request for the purpose of ensuring that the consumer's personal information remains deleted from the business's records.
- (6) In cases where a business denies a consumer's request to delete, the business shall do all of the following:

 - a. Inform the consumer that it will not comply with the consumer's request and describe the basis for the denial, including any conflict with federal or state law, or exception to the CCPA, unless prohibited from doing so by law;
 - b. Delete the consumer's personal information that is not subject to the exception; and
 - c. Not use the consumer's personal information retained for any other purpose than provided for by that exception.
- (7) If a business that denies a consumer's request to delete sells personal information and the consumer has not already made a request to opt-out, the business shall ask the consumer if they would like to opt-out of the sale of their personal information and

shall include either the contents of, or a link to, the notice of right to opt-out in accordance with section 999.306.

- (8) In responding to a request to delete, a business may present the consumer with the choice to delete select portions of their personal information only if a global option to delete all personal information is also offered and more prominently presented than the other choices.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.110, 1798.115, 1798.130 and 1798.185, Civil Code.

§ 999.314. Service Providers.

- (a) A business that provides services to a person or organization that is not a business, and that would otherwise meet the requirements and obligations of a “service provider” under the CCPA and these regulations, shall be deemed a service provider for purposes of the CCPA and these regulations.
- (b) To the extent that a business directs a second entity to collect personal information directly from a consumer, or about a consumer, on the first business’s behalf, and the second entity would otherwise meet the requirements and obligations of a “service provider” under the CCPA and these regulations, the second entity shall be deemed a service provider of the first business for purposes of the CCPA and these regulations.
- (c) A service provider shall not retain, use, or disclose personal information obtained in the course of providing services except:
- (1) To process or maintain personal information on behalf of the business that provided the personal information or directed the service provider to collect the personal information, and in compliance with the written contract for services required by the CCPA;
 - (2) To retain and employ another service provider as a subcontractor, where the subcontractor meets the requirements for a service provider under the CCPA and these regulations;
 - (3) For internal use by the service provider to build or improve the quality of its services, provided that the use does not include building or modifying household or consumer profiles to use in providing services to another business, or correcting or augmenting data acquired from another source;
 - (4) To detect data security incidents or protect against fraudulent or illegal activity; or
 - (5) For the purposes enumerated in Civil Code section 1798.145, subdivisions (a)(1) through (a)(4).
- (d) A service provider shall not sell data on behalf of a business when a consumer has opted-out of the sale of their personal information with the business.

- (e) If a service provider receives a request to know or a request to delete from a consumer, the service provider shall either act on behalf of the business in responding to the request or inform the consumer that the request cannot be acted upon because the request has been sent to a service provider.
- (f) A service provider that is a business shall comply with the CCPA and these regulations with regard to any personal information that it collects, maintains, or sells outside of its role as a service provider.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.110, 1798.115, 1798.130, 1798.140 and 1798.185, Civil Code.

§ 999.315. Requests to Opt-Out.

- (a) A business shall provide two or more designated methods for submitting requests to opt-out, including an interactive form accessible via a clear and conspicuous link titled “Do Not Sell My Personal Information,” on the business’s website or mobile application. Other acceptable methods for submitting these requests include, but are not limited to, a toll-free phone number, a designated email address, a form submitted in person, a form submitted through the mail, and user-enabled global privacy controls, such as a browser plug-in or privacy setting, device setting, or other mechanism, that communicate or signal the consumer’s choice to opt-out of the sale of their personal information.
- (b) A business shall consider the methods by which it interacts with consumers, the manner in which the business sells personal information to third parties, available technology, and ease of use by the consumer when determining which methods consumers may use to submit requests to opt-out. At least one method offered shall reflect the manner in which the business primarily interacts with the consumer.
- (c) If a business collects personal information from consumers online, the business shall treat user-enabled global privacy controls, such as a browser plug-in or privacy setting, device setting, or other mechanism, that communicate or signal the consumer’s choice to opt-out of the sale of their personal information as a valid request submitted pursuant to Civil Code section 1798.120 for that browser or device, or, if known, for the consumer.
 - (1) Any privacy control developed in accordance with these regulations shall clearly communicate or signal that a consumer intends to opt-out of the sale of personal information.
 - (2) If a global privacy control conflicts with a consumer’s existing business-specific privacy setting or their participation in a business’s financial incentive program, the business shall respect the global privacy control but may notify the consumer of the conflict and give the consumer the choice to confirm the business-specific privacy setting or participation in the financial incentive program.
- (d) In responding to a request to opt-out, a business may present the consumer with the choice to opt-out of sale for certain uses of personal information as long as a global option to opt-

out of the sale of all personal information is more prominently presented than the other choices.

- (e) A business shall comply with a request to opt-out as soon as feasibly possible, but no later than 15 business days from the date the business receives the request. If a business sells a consumer's personal information to any third parties after the consumer submits their request but before the business complies with that request, it shall notify those third parties that the consumer has exercised their right to opt-out and shall direct those third parties not to sell that consumer's information.
- (f) A consumer may use an authorized agent to submit a request to opt-out on the consumer's behalf if the consumer provides the authorized agent written permission signed by the consumer. A business may deny a request from an authorized agent if the agent cannot provide to the business the consumer's signed permission demonstrating that they have been authorized by the consumer to act on the consumer's behalf. User-enabled global privacy controls, such as a browser plug-in or privacy setting, device setting, or other mechanism, that communicate or signal the consumer's choice to opt-out of the sale of their personal information shall be considered a request directly from the consumer, not through an authorized agent.
- (g) A request to opt-out need not be a verifiable consumer request. If a business, however, has a good-faith, reasonable, and documented belief that a request to opt-out is fraudulent, the business may deny the request. The business shall inform the requestor that it will not comply with the request and shall provide an explanation why it believes the request is fraudulent.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.120, 1798.135, 1798.140 and 1798.185, Civil Code.

§ 999.316. Requests to Opt-In After Opting-Out of the Sale of Personal Information.

- (a) Requests to opt-in to the sale of personal information shall use a two-step opt-in process whereby the consumer shall first, clearly request to opt-in and then second, separately confirm their choice to opt-in.
- (b) If a consumer who has opted-out of the sale of their personal information initiates a transaction or attempts to use a product or service that requires the sale of their personal information, a business may inform the consumer that the transaction, product, or service requires the sale of their personal information and provide instructions on how the consumer can opt-in.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.120, 1798.135 and 1798.185, Civil Code.

§ 999.317. Training; Record-Keeping.

- (a) All individuals responsible for handling consumer inquiries about the business's privacy practices or the business's compliance with the CCPA shall be informed of all of the

requirements in the CCPA and these regulations and how to direct consumers to exercise their rights under the CCPA and these regulations.

- (b) A business shall maintain records of consumer requests made pursuant to the CCPA and how it responded to the requests for at least 24 months. The business shall implement and maintain reasonable security procedures and practices in maintaining these records.
- (c) The records may be maintained in a ticket or log format provided that the ticket or log includes the date of request, nature of request, manner in which the request was made, the date of the business's response, the nature of the response, and the basis for the denial of the request if the request is denied in whole or in part.
- (d) A business's maintenance of the information required by this section, where that information is not used for any other purpose, does not taken alone violate the CCPA or these regulations.
- (e) Information maintained for record-keeping purposes shall not be used for any other purpose except as reasonably necessary for the business to review and modify its processes for compliance with the CCPA and these regulations. Information maintained for record-keeping purposes shall not be shared with any third party except as necessary to comply with a legal obligation.
- (f) Other than as required by subsection (b), a business is not required to retain personal information solely for the purpose of fulfilling a consumer request made under the CCPA.
- (g) A business that knows or reasonably should know that it, alone or in combination, buys, receives for the business's commercial purposes, sells, or shares for commercial purposes the personal information of 10,000,000 or more consumers in a calendar year shall:

 - (1) Compile the following metrics for the previous calendar year:

 - a. The number of requests to know that the business received, complied with in whole or in part, and denied;
 - b. The number of requests to delete that the business received, complied with in whole or in part, and denied;
 - c. The number of requests to opt-out that the business received, complied with in whole or in part, and denied; and
 - d. The median or mean number of days within which the business substantively responded to requests to know, requests to delete, and requests to opt-out.
 - (2) Disclose, by July 1 of every calendar year, the information compiled in subsection (g)(1) within their privacy policy or posted on their website and accessible from a link included in their privacy policy.

- a. In its disclosure pursuant to subsection (g)(2), a business may choose to disclose the number of requests that it denied in whole or in part because the request was not verifiable, was not made by a consumer, called for information exempt from disclosure, or was denied on other grounds.
- (3) Establish, document, and comply with a training policy to ensure that all individuals responsible for handling consumer requests made under the CCPA or the business's compliance with the CCPA are informed of all the requirements in these regulations and the CCPA.
- (h) A business may choose to compile and disclose the information required by subsection (g)(1) for requests received from all individuals, rather than requests received from consumers. The business shall state whether it has done so in its disclosure and shall, upon request, compile and provide to the Attorney General the information required by subsection (g)(1) for requests received from consumers.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.110, 1798.115, 1798.120, 1798.130, 1798.135 and 1798.185, Civil Code.

§ 999.318. Requests to Know or Delete Household Information.

- (a) Where a household does not have a password-protected account with a business, a business shall not comply with a request to know specific pieces of personal information about the household or a request to delete household personal information unless all of the following conditions are satisfied:
 - (1) All consumers of the household jointly request to know specific pieces of information for the household or the deletion of household personal information;
 - (2) The business individually verifies all the members of the household subject to the verification requirements set forth in section 999.325; and
 - (3) The business verifies that each member making the request is currently a member of the household.
- (b) Where a consumer has a password-protected account with a business that collects personal information about a household, the business may process requests to know and requests to delete relating to household information through the business's existing business practices and in compliance with these regulations.
- (c) If a member of a household is a consumer under the age of 13, a business must obtain verifiable parental consent before complying with a request to know specific pieces of information for the household or the deletion of household personal information pursuant to the parental consent provisions in section 999.330.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Section 1798.100, 1798.105, 1798.110, 1798.115, 1798.120, 1798.130, 1798.140 and 1798.185, Civil Code.

Article 4. VERIFICATION OF REQUESTS

§ 999.323. General Rules Regarding Verification.

- (a) A business shall establish, document, and comply with a reasonable method for verifying that the person making a request to know or a request to delete is the consumer about whom the business has collected information.
- (b) In determining the method by which the business will verify the consumer's identity, the business shall:

 - (1) Whenever feasible, match the identifying information provided by the consumer to the personal information of the consumer already maintained by the business, or use a third-party identity verification service that complies with this section.
 - (2) Avoid collecting the types of personal information identified in Civil Code section 1798.81.5, subdivision (d), unless necessary for the purpose of verifying the consumer.
 - (3) Consider the following factors:

 - a. The type, sensitivity, and value of the personal information collected and maintained about the consumer. Sensitive or valuable personal information shall warrant a more stringent verification process. The types of personal information identified in Civil Code section 1798.81.5, subdivision (d), shall be considered presumptively sensitive;
 - b. The risk of harm to the consumer posed by any unauthorized access or deletion. A greater risk of harm to the consumer by unauthorized access or deletion shall warrant a more stringent verification process;
 - c. The likelihood that fraudulent or malicious actors would seek the personal information. The higher the likelihood, the more stringent the verification process shall be;
 - d. Whether the personal information to be provided by the consumer to verify their identity is sufficiently robust to protect against fraudulent requests or being spoofed or fabricated;
 - e. The manner in which the business interacts with the consumer; and
 - f. Available technology for verification.
- (c) A business shall generally avoid requesting additional information from the consumer for purposes of verification. If, however, the business cannot verify the identity of the consumer from the information already maintained by the business, the business may request additional information from the consumer, which shall only be used for the purposes of verifying the identity of the consumer seeking to exercise their rights under the CCPA.

security, or fraud-prevention. The business shall delete any new personal information collected for the purposes of verification as soon as practical after processing the consumer's request, except as required to comply with section 999.317.

- (d) A business shall not require the consumer or the consumer's authorized agent to pay a fee for the verification of their request to know or request to delete. For example, a business may not require a consumer to provide a notarized affidavit to verify their identity unless the business compensates the consumer for the cost of notarization.
- (e) A business shall implement reasonable security measures to detect fraudulent identity-verification activity and prevent the unauthorized access to or deletion of a consumer's personal information.
- (f) If a business maintains consumer information that is deidentified, a business is not obligated to provide or delete this information in response to a consumer request or to re-identify individual data to verify a consumer request.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.110, 1798.115, 1798.130, 1798.140 and 1798.185, Civil Code.

§ 999.324. Verification for Password-Protected Accounts.

- (a) If a business maintains a password-protected account with the consumer, the business may verify the consumer's identity through the business's existing authentication practices for the consumer's account, provided that the business follows the requirements in section 999.323. The business shall also require a consumer to re-authenticate themselves before disclosing or deleting the consumer's data.
- (b) If a business suspects fraudulent or malicious activity on or from the password-protected account, the business shall not comply with a consumer's request to know or request to delete until further verification procedures determine that the consumer request is authentic and the consumer making the request is the person about whom the business has collected information. The business may use the procedures set forth in section 999.325 to further verify the identity of the consumer.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.110, 1798.115, 1798.130 and 1798.185, Civil Code.

§ 999.325. Verification for Non-Accountholders.

- (a) If a consumer does not have or cannot access a password-protected account with a business, the business shall comply with this section, in addition to section 999.323.
- (b) A business's compliance with a request to know categories of personal information requires that the business verify the identity of the consumer making the request to a reasonable degree of certainty. A reasonable degree of certainty may include matching at least two data

points provided by the consumer with data points maintained by the business that it has determined to be reliable for the purpose of verifying the consumer.

- (c) A business's compliance with a request to know specific pieces of personal information requires that the business verify the identity of the consumer making the request to a reasonably high degree of certainty. A reasonably high degree of certainty may include matching at least three pieces of personal information provided by the consumer with personal information maintained by the business that it has determined to be reliable for the purpose of verifying the consumer together with a signed declaration under penalty of perjury that the requestor is the consumer whose personal information is the subject of the request. If a business uses this method for verification, the business shall maintain all signed declarations as part of its record-keeping obligations.
- (d) A business's compliance with a request to delete may require that the business verify the identity of the consumer to a reasonable or reasonably high degree of certainty depending on the sensitivity of the personal information and the risk of harm to the consumer posed by unauthorized deletion. For example, the deletion of family photographs may require a reasonably high degree of certainty, while the deletion of browsing history may require only a reasonable degree of certainty. A business shall act in good faith when determining the appropriate standard to apply when verifying the consumer in accordance with these regulations.
- (e) Illustrative examples follow:
 - (1) Example 1: If a business maintains personal information in a manner associated with a named actual person, the business may verify the consumer by requiring the consumer to provide evidence that matches the personal information maintained by the business. For example, if a retailer maintains a record of purchases made by a consumer, the business may require the consumer to identify items that they recently purchased from the store or the dollar amount of their most recent purchase to verify their identity to a reasonable degree of certainty.
 - (2) Example 2: If a business maintains personal information in a manner that is not associated with a named actual person, the business may verify the consumer by requiring the consumer to demonstrate that they are the sole consumer associated with the personal information. For example, a business may have a mobile application that collects personal information about the consumer but does not require an account. The business may determine whether, based on the facts and considering the factors set forth in section 999.323, subsection (b)(3), it may reasonably verify a consumer by asking them to provide information that only the person who used the mobile application may know or by requiring the consumer to respond to a notification sent to their device.
- (f) A business shall deny a request to know specific pieces of personal information if it cannot verify the identity of the requestor pursuant to these regulations.

- (g) If there is no reasonable method by which a business can verify the identity of the consumer to the degree of certainty required by this section, the business shall state so in response to any request and explain why it has no reasonable method by which it can verify the identity of the requestor. If the business has no reasonable method by which it can verify any consumer, the business shall explain why it has no reasonable verification method in its privacy policy. The business shall evaluate and document whether a reasonable method can be established at least once every 12 months, in connection with the requirement to update the privacy policy set forth in Civil Code section 1798.130, subdivision (a)(5).

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.110, 1798.115, 1798.130 and 1798.185, Civil Code.

§ 999.326. Authorized Agent.

- (a) When a consumer uses an authorized agent to submit a request to know or a request to delete, a business may require that the consumer do the following:
- (1) Provide the authorized agent signed permission to do so.
 - (2) Verify their own identity directly with the business.
 - (3) Directly confirm with the business that they provided the authorized agent permission to submit the request.
- (b) Subsection (a) does not apply when a consumer has provided the authorized agent with power of attorney pursuant to Probate Code sections 4121 to 4130.
- (c) An authorized agent shall implement and maintain reasonable security procedures and practices to protect the consumer's information.
- (d) An authorized agent shall not use a consumer's personal information, or any information collected from or about the consumer, for any purposes other than to fulfill the consumer's requests, verification, or fraud prevention.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.110, 1798.115, 1798.130 and 1798.185, Civil Code.

Article 5. SPECIAL RULES REGARDING CONSUMERS UNDER 16 YEARS OF AGE

§ 999.330. Consumers Under 13 Years of Age.

- (a) Process for Opting-In to Sale of Personal Information
- (1) A business that has actual knowledge that it sells the personal information of a consumer under the age of 13 shall establish, document, and comply with a reasonable method for determining that the person affirmatively authorizing the sale of the personal information about the child is the parent or guardian of that child. This

affirmative authorization is in addition to any verifiable parental consent required under COPPA.

- (2) Methods that are reasonably calculated to ensure that the person providing consent is the child's parent or guardian include, but are not limited to:
- a. Providing a consent form to be signed by the parent or guardian under penalty of perjury and returned to the business by postal mail, facsimile, or electronic scan;
 - b. Requiring a parent or guardian, in connection with a monetary transaction, to use a credit card, debit card, or other online payment system that provides notification of each discrete transaction to the primary account holder;
 - c. Having a parent or guardian call a toll-free telephone number staffed by trained personnel;
 - d. Having a parent or guardian connect to trained personnel via video-conference;
 - e. Having a parent or guardian communicate in person with trained personnel; and
 - f. Verifying a parent or guardian's identity by checking a form of government-issued identification against databases of such information, as long as the parent or guardian's identification is deleted by the business from its records promptly after such verification is complete.
- (b) When a business receives an affirmative authorization pursuant to subsection (a), the business shall inform the parent or guardian of the right to opt-out and of the process for doing so on behalf of their child pursuant to section 999.315, subsections (a)-(f).
- (c) A business shall establish, document, and comply with a reasonable method, in accordance with the methods set forth in subsection (a)(2), for determining that a person submitting a request to know or a request to delete the personal information of a child under the age of 13 is the parent or guardian of that child.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.120, 1798.135 and 1798.185, Civil Code.

§ 999.331. Consumers 13 to 15 Years of Age.

- (a) A business that has actual knowledge that it sells the personal information of consumers at least 13 years of age and less than 16 years of age shall establish, document, and comply with a reasonable process for allowing such consumers to opt-in to the sale of their personal information, pursuant to section 999.316.
- (b) When a business receives a request to opt-in to the sale of personal information from a consumer at least 13 years of age and less than 16 years of age, the business shall inform the

consumer of the right to opt-out at a later date and of the process for doing so pursuant to section 999.315.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.120, 1798.135 and 1798.185, Civil Code.

§ 999.332. Notices to Consumers Under 16 Years of Age.

- (a) A business subject to sections 999.330 and 999.331 shall include a description of the processes set forth in those sections in its privacy policy.
- (b) A business that exclusively targets offers of goods or services directly to consumers under 16 years of age and does not sell the personal information without the affirmative authorization of consumers at least 13 years of age and less than 16 years of age, or the affirmative authorization of their parent or guardian for consumers under 13 years of age, is not required to provide the notice of right to opt-out.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.120, 1798.135 and 1798.185, Civil Code.

Article 6. NON-DISCRIMINATION

§ 999.336. Discriminatory Practices.

- (a) A financial incentive or a price or service difference is discriminatory, and therefore prohibited by Civil Code section 1798.125, if the business treats a consumer differently because the consumer exercised a right conferred by the CCPA or these regulations.
- (b) A business may offer a financial incentive or price or service difference if it is reasonably related to the value of the consumer's data. If a business is unable to calculate a good-faith estimate of the value of the consumer's data or cannot show that the financial incentive or price or service difference is reasonably related to the value of the consumer's data, that business shall not offer the financial incentive or price or service difference.
- (c) A business's denial of a consumer's request to know, request to delete, or request to opt-out for reasons permitted by the CCPA or these regulations shall not be considered discriminatory.
- (d) Illustrative examples follow:
 - (1) *Example 1:* A music streaming business offers a free service as well as a premium service that costs \$5 per month. If only the consumers who pay for the music streaming service are allowed to opt-out of the sale of their personal information, then the practice is discriminatory, unless the \$5-per-month payment is reasonably related to the value of the consumer's data to the business.

(2) Example 2: A clothing business offers a loyalty program whereby customers receive a \$5-off coupon by email after spending \$100 with the business. A consumer submits a request to delete all personal information the business has collected about them but also informs the business that they want to continue to participate in the loyalty program. The business may deny their request to delete with regard to their email address and the amount the consumer has spent with the business because that information is necessary for the business to provide the loyalty program requested by the consumer and is reasonably anticipated within the context of the business's ongoing relationship with them pursuant to Civil Code section 1798.105, subdivision (d)(1).

(3) Example 3: A grocery store offers a loyalty program whereby consumers receive coupons and special discounts when they provide their phone numbers. A consumer submits a request to opt-out of the sale of their personal information. The retailer complies with their request but no longer allows the consumer to participate in the loyalty program. This practice is discriminatory unless the grocery store can demonstrate that the value of the coupons and special discounts are reasonably related to the value of the consumer's data to the business.

(4) Example 4: An online bookseller collects information about consumers, including their email addresses. It offers coupons to consumers through browser pop-up windows while the consumer uses the bookseller's website. A consumer submits a request to delete all personal information that the bookseller has collected about them, including their email address and their browsing and purchasing history. The bookseller complies with the request but stops providing the periodic coupons to the consumer. The bookseller's failure to provide coupons is discriminatory unless the value of the coupons is reasonably related to the value provided to the business by the consumer's data. The bookseller may not deny the consumer's request to delete with regard to the email address because the email address is not necessary to provide the coupons or reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business.

(e) A business shall notify consumers of any financial incentive or price or service difference subject to Civil Code section 1798.125 that it offers in accordance with section 999.307.

(f) A business's charging of a reasonable fee pursuant to Civil Code section 1798.145, subdivision (i)(3), shall not be considered a financial incentive subject to these regulations.

(g) A price or service difference that is the direct result of compliance with a state or federal law shall not be considered discriminatory.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.125, 1798.130 and 1798.185, Civil Code.

§ 999.337. Calculating the Value of Consumer Data

- (a) A business offering a financial incentive or price or service difference subject to Civil Code section 1798.125 shall use and document a reasonable and good faith method for calculating the value of the consumer's data. The business shall consider one or more of the following:
- (1) The marginal value to the business of the sale, collection, or deletion of a consumer's data.
 - (2) The average value to the business of the sale, collection, or deletion of a consumer's data.
 - (3) The aggregate value to the business of the sale, collection, or deletion of consumers' data divided by the total number of consumers.
 - (4) Revenue generated by the business from sale, collection, or retention of consumers' personal information.
 - (5) Expenses related to the sale, collection, or retention of consumers' personal information.
 - (6) Expenses related to the offer, provision, or imposition of any financial incentive or price or service difference.
 - (7) Profit generated by the business from sale, collection, or retention of consumers' personal information.
 - (8) Any other practical and reasonably reliable method of calculation used in good faith.
- (b) For the purpose of calculating the value of consumer data, a business may consider the value to the business of the data of all natural persons in the United States and not just consumers.


Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.125, 1798.130 and 1798.185, Civil Code.

Conn. Gen. Stat. § 36a-701b

Current through 20-1 of the 2020 First Regular Session, and 20-4 of the July Special Session.

LexisNexis® Connecticut Annotated Statutes > Title 36a The Banking Law of Connecticut (Chs. 664 — 669) > Chapter 669 Regulated Activities (Pts. I — XIV) > Part V Consumer Credit Reports (§§ 36a-695 — 36a-704)

Notice

 This section has more than one version with varying effective dates.

Sec. 36a-701b. Breach of security re computerized data containing personal information. Notice of breach. Provision of identity theft prevention services and identity theft mitigation services. Delay for criminal investigation. Means of notice. Unfair trade practice. [Effective October 1, 2021]

(a) For purposes of this section, (1) “breach of security” means unauthorized access to or unauthorized acquisition of electronic files, media, databases or computerized data, containing personal information when access to the personal information has not been secured by encryption or by any other method or technology that renders the personal information unreadable or unusable; and (2) “personal information” means an individual’s first name or first initial and last name in combination with any one, or more, of the following data: (A) Social Security number; (B) driver’s license number or state identification card number; (C) credit or debit card number; or (D) financial account number in combination with any required security code, access code or password that would permit access to such financial account. “Personal information” does not include publicly available information that is lawfully made available to the general public from federal, state or local government records or widely distributed media.

(b)

(1) Any person who conducts business in this state, and who, in the ordinary course of such person’s business, owns, licenses or maintains computerized data that includes personal information, shall provide notice of any breach of security following the discovery of the breach to any resident of this state whose personal information was breached or is reasonably believed to have been breached. Such notice shall be made without unreasonable delay but not later than ninety days after the discovery of such breach, unless a shorter time is required under federal law, subject to the provisions of subsection (d) of this section and the completion of an investigation by such person to determine the nature and scope of the incident, to identify the individuals affected, or to restore the reasonable integrity of the data system. Such notification shall not be required if, after an appropriate investigation and consultation with relevant federal, state and local agencies responsible for law enforcement, the person reasonably determines that the breach will not likely result in harm to the individuals whose personal information has been acquired and accessed.

(2) If notice of a breach of security is required by subdivision (1) of this subsection:

(A) The person who conducts business in this state, and who, in the ordinary course of such person’s business, owns, licenses or maintains computerized data that includes personal

information, shall, not later than the time when notice is provided to the resident, also provide notice of the **breach** of security to the Attorney General; and

(B) The person who conducts business in this state, and who, in the ordinary course of such person's business, owns or licenses computerized data that includes personal information, shall offer to each resident whose nonpublic information under subparagraph (B)(i) of subdivision (9) of subsection (b) of section 38a-38 or personal information as defined in subparagraph (A) of subdivision (2) of subsection (a) of this section was **breached** or is reasonably believed to have been **breached**, appropriate identity theft prevention services and, if applicable, identity theft mitigation services. Such service or services shall be provided at no cost to such resident for a period of not less than twenty-four months. Such person shall provide all information necessary for such resident to enroll in such service or services and shall include information on how such resident can place a credit freeze on such resident's credit file.

(c) Any person that maintains computerized data that includes personal information that the person does not own shall notify the owner or licensee of the information of any **breach** of the security of the data immediately following its discovery, if the personal information of a resident of this state was **breached** or is reasonably believed to have been **breached**.

(d) Any **notification** required by this section shall be delayed for a reasonable period of time if a law enforcement agency determines that the **notification** will impede a criminal investigation and such law enforcement agency has made a request that the **notification** be delayed. Any such delayed **notification** shall be made after such law enforcement agency determines that **notification** will not compromise the criminal investigation and so notifies the person of such determination.

(e) Any notice to a resident, owner or licensee required by the provisions of this section may be provided by one of the following methods: (1) Written notice; (2) telephone notice; (3) electronic notice, provided such notice is consistent with the provisions regarding electronic records and signatures set forth in [15 USC 7001](#); (4) substitute notice, provided such person demonstrates that the cost of providing notice in accordance with subdivision (1), (2) or (3) of this subsection would exceed two hundred fifty thousand dollars, that the affected class of subject persons to be notified exceeds five hundred thousand persons or that the person does not have sufficient contact information. Substitute notice shall consist of the following: (A) Electronic mail notice when the person has an electronic mail address for the affected persons; (B) conspicuous posting of the notice on the web site of the person if the person maintains one; and (C) **notification** to major state-wide media, including newspapers, radio and television.

(f) Any person that maintains such person's own security **breach** procedures as part of an information security policy for the treatment of personal information and otherwise complies with the timing requirements of this section, shall be deemed to be in compliance with the security **breach notification** requirements of this section, provided such person notifies, as applicable, residents of this state, owners and licensees in accordance with such person's policies in the event of a **breach** of security and in the case of notice to a resident, such person also notifies the Attorney General not later than the time when notice is provided to the resident. Any person that maintains such a security **breach** procedure pursuant to the rules, regulations, procedures or guidelines established by the primary or functional regulator, as defined in [15 USC 6809\(2\)](#), shall be deemed to be in compliance with the security **breach notification** requirements of this section, provided (1) such person notifies, as applicable, such residents of this state, owners, and licensees required to be notified under and in accordance with the policies or the rules, regulations, procedures or guidelines established by the primary or functional regulator in the event of a **breach** of security, and (2) if notice is given to a resident of this state in accordance with subdivision (1) of this subsection regarding a **breach** of security, such person also notifies the Attorney General not later than the time when notice is provided to the resident.

(g) Failure to comply with the requirements of this section shall constitute an unfair trade practice for purposes of [section 42-110b](#) and shall be enforced by the Attorney General.

History

[P.A. 05-148, S. 3](#); [05-288, S. 231](#), 232; June 12 Sp. Sess. [P.A. 12-1, S. 130](#), eff. Oct. 1, 2012; [P.A. 15-142, S. 6](#), eff. Oct. 1, 2015; [P.A. 18-90, S. 2](#), eff. Oct. 1, 2018; [P.A. 19-117, S. 231](#), eff. Oct. 1, 2020.

Annotations

Notes

Amendment Notes

2015 amendment, by P.A. 15-142, effective Oct. 1, 2015, in the first sentence of (a), in the opening language, inserted the (1) and (2) designations and inserted the serial comma following “computerized data”, and in (2), redesignated former subdivisions (1) through (3) as subdivisions (A) through (C); in (b)(1), substituted “personal information was ***breached*** or is reasonably believed to have been ***breached***” for “personal information was, or is reasonably believed to have been, accessed by an unauthorized person through such ***breach*** of security” in the first sentence, and inserted “but not later than ninety days after the discovery of such ***breach***, unless a shorter time is required under federal law” in the second sentence; added the (b)(2)(A) designation; added (b)(2)(B); substituted “this state was ***breached*** or is reasonably believed to have been ***breached***” for “this state was, or is reasonably believed to have been accessed by an unauthorized person” in (c); and made related changes.

2018 amendment, by P.A. 18-90, effective Oct. 1, 2018, in the first sentence of (a), deleted “or” following “identification card number,” “account number” preceding “credit or debit” in subdivision (2)(C), added the (2)(D) designation, in (2)(D), added “financial account number” and substituted “such” for “an individual’s”; and substituted “twenty-four months” for “twelve months” in the second sentence of (a)(2)(B).

2019 amendment, by P.A. 19-117, effective Oct. 1, 2021, substituted “nonpublic information under subparagraph (B)(i) of subdivision (9) of subsection (b) of section 230 of this act or personal information as defined in” for “personal information under subparagraph (A) of subdivision (4) of subsection (a) of section 38a-999b or” in the first sentence of (b)(2)(B).

Research References & Practice Aids

Hierarchy Notes:

[Conn. Gen. Stat. Title 36a](#)

[Conn. Gen. Stat. Title 36a, Ch. 669](#)

State Notes

Notes

History Notes:

[P.A. 05-148](#) effective January 1, 2006; [P.A. 05-288](#) made technical changes in Subsecs. (b) and (f), effective January 1, 2006; June 12 Sp. Sess. *P.A. 12-1* amended Subsec. (a) by adding “unauthorized” re acquisition, amended Subsec. (b) by designating existing provisions as Subdiv. (1) and amending same to replace “disclose” with “provide notice of” and “disclosure” with “notice” and by adding Subdiv. (2) re notice of ***breach*** of security to Attorney General, amended Subsec. (c) by adding “of a resident of this state” re personal information, amended Subsec. (e) by adding “to a resident, owner or licensee” re notice, replacing “person, business or agency” with “person” and making a technical change, and amended Subsec. (f) by replacing references to subject persons with references to residents of this state, owners and licensees, as applicable, adding provisions re notice to Attorney General and deleting reference to system.

LexisNexis® Connecticut Annotated Statutes

Copyright © 2020 Matthew Bender & Company, Inc. a member of the LexisNexis Group. All rights reserved.

End of Document

D.C. Code § 28-3852

The Official Code is current through Oct. 20, 2020

District of Columbia Official Code > Division V. Local Business Affairs. (Titles 25 — 37) > Title 28. Commercial Instruments and Transactions. (Subts. I — II) > Subtitle II. Other Commercial Transactions. (Chs. 21 — 53) > Chapter 38. Consumer Protections. (Subchs. I — III) > Subchapter II. Consumer Security Breach Notification. (§§ 28-3851 — 28-3853)

§ 28-3852. Notification of security breach.

(a) Any person or entity who conducts business in the District of Columbia, and who, in the course of such business, owns or licenses computerized or other electronic data that includes personal information, and who discovers a **breach** of the security of the system, shall promptly notify any District of Columbia resident whose personal information was included in the **breach**. The **notification** shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection (d) of this section, and with any measures necessary to determine the scope of the **breach** and restore the reasonable integrity of the data system.

(a-1) The **notification** required under subsection (a) of this section shall include:

- (1) To the extent possible, a description of the categories of information that were, or are reasonably believed to have been, acquired by an unauthorized person, including the elements of personal information that were, or are reasonably believed to have been, acquired;
- (2) Contact information for the person or entity making the **notification**, including the business address, telephone number, and toll-free telephone number if one is maintained;
- (3) The toll-free telephone numbers and addresses for the major consumer reporting agencies, including a statement notifying the resident of the right to obtain a security freeze free of charge pursuant to 15 U.S.C. § 1681c-1 and information how a resident may request a security freeze; and
- (4) The toll-free telephone numbers, addresses, and website addresses for the following entities, including a statement that an individual can obtain information from these sources about steps to take to avoid identity theft:

(A) The Federal Trade Commission; and

(B) The Office of the Attorney General for the District of Columbia.

(a-2) Notwithstanding subsection (a-1) of this section, in the case of a **breach** of the security of the system that only involves personal information as defined in § 28-3851(3)(A)(ii), the person or entity may comply with this section by providing the **notification** in electronic format or other form that directs the person to change the person's password and security question or answer, as applicable, or to take other steps appropriate to protect the e-mail account with the person or entity and all other online accounts for which the person whose personal information has been **breached** uses the same username or email address and password or security question or answer.

(b) Any person or entity who maintains, handles, or otherwise possesses computerized or other electronic data that includes personal information that the person or entity does not own shall notify the owner or licensee of the information of any **breach** of the security of the system in the most expedient time possible following discovery.

(b-1) In addition to giving the **notification** required under subsection (a) of this section, and subject to subsection (d) of this section, the person or entity required to give notice shall promptly provide written notice of

the **breach** of the security of the system to the Office of the Attorney General for the District of Columbia if the **breach** affects 50 or more District residents. This notice shall be made in the most expedient manner possible, without unreasonable delay, and in no event later than when notice is provided under subsection (a) of this section. The written notice shall include:

- (1)The name and contact information of the person or entity reporting the **breach**;
- (2)The name and contact information of the person or entity that experienced the **breach**;
- (3)The nature of the **breach** of the security of the system, including the name of the person or entity that experienced the **breach**;
- (4)The types of personal information compromised by the **breach**;
- (5)The number of District residents affected by the **breach**;
- (6)The cause of the **breach**, including the relationship between the person or entity that experienced the **breach** and the person responsible for the **breach**, if known;
- (7)The remedial action taken by the person or entity to include steps taken to assist District residents affected by the **breach**;
- (8)The date and time frame of the **breach**, if known;
- (9)The address and location of corporate headquarters, if outside of the District;
- (10)Any knowledge of foreign country involvement; and
- (11)A sample of the notice to be provided to District residents.

(b-2)The notice required under subsection (b-1) of this section shall not be delayed on the grounds that the total number of District residents affected by the **breach** has not yet been ascertained.

(c)If any person or entity is required by subsection (a) or (b) of this section to notify more than 1,000 persons of a **breach** of security pursuant to this subsection, the person shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined by section 603(p) of the Fair Credit Reporting Act, approved October 26, 1970 (84 Stat. 1128; 15 U.S.C. § [1681a\(p\)](#)), of the timing, distribution and content of the notices. Nothing in this subsection shall be construed to require the person to provide to the consumer reporting agency the names or other personal identifying information of **breach** notice recipients. This subsection shall not apply to a person or entity who is required to notify consumer reporting agencies of a **breach** pursuant to Title V of the Gramm-Leach-Bliley Act, approved November 12, 1999 (113 Stat. 1436; 15 U.S.C. § [6801](#) et seq[.]).

(d)The **notification** required by this section may be delayed if a law enforcement agency determines that the **notification** will impede a criminal investigation but shall be made as soon as possible after the law enforcement agency determines that the **notification** will not compromise the investigation.

(e)[Repealed].

(f)A waiver of any provision of this subchapter shall be void and unenforceable.

(g)A person or entity that maintains procedures for a **breach notification** system under Title V of the Gramm-Leach-Bliley Act, approved November 12, 1999 (113 Stat. 1436; 15 U.S.C. § 6801 et seq.), or the **breach notification** rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability Accountability Act of 1996, approved August 21, 1996 (Pub. L. No. 104-191; 110 Stat. 1936), or the Health Information Technology for Economic and Clinical Health Act, approved February 17, 2009 (Pub. L. No. 111-5; 123 Stat. 226), and provides notice in accordance with such Acts, and any rules, regulations, guidance and guidelines thereto, to each affected resident in the event of a **breach**, shall be deemed to be in compliance with this section with respect to the **notification** of residents whose personal information is included in the **breach**. The person or entity shall, in all cases, provide written notice of the **breach** of the security of the system to the Office of the Attorney General for the District of Columbia as required under subsection (b-1) of this section.

History

(Mar. 8, 2007, D.C. Law 16-237, § 2(c), [54 DCR 393](#); June 17, 2020, D.C. Law 23-98, § 2(a)(4), [67 DCR 3923](#).)

Annotations

Notes

Effect of amendments.

The 2020 amendment by D.C. Law 23-98 added (a-1), (a-2), (b-1), and (b-2); repealed (e); and rewrote (g).

Legislative history of Law 16-237.

For Law 16-237, see notes following § 28-3851.

Legislative history of Law 23-98.

See note to § 28-3851.

Research References & Practice Aids

LAW REVIEWS AND JOURNAL COMMENTARIES

Comment: Giving Consumers a Leg to Stand on: Finding Plaintiffs a Legislative Solution to the Barrier from Federal Courts in Data Security ***Breach*** Suits, [62 Cath. U.L. Rev. 765 \(2013\)](#).

District of Columbia Official Code
Copyright © 2020 All rights reserved.

End of Document

815 ILCS 530/10

Statutes current with legislation through P.A. 101-650 of the 2020 Session of the 101st Legislature.

Illinois Compiled Statutes Annotated > Chapter 815 BUSINESS TRANSACTIONS (§§ 5/1 — 730/99) > DECEPTIVE PRACTICES (§§ 505/1 — 603/99) > Personal Information Protection Act (§§ 530/1 — 530/900)

815 ILCS 530/10 Notice of breach; notice to Attorney General.

(a)Any data collector that owns or licenses personal information concerning an Illinois resident shall notify the resident at no charge that there has been a breach of the security of the system data following discovery or notification of the breach. The disclosure notification shall be made in the most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system. The disclosure notification to an Illinois resident shall include, but need not be limited to, information as follows:

(1)With respect to personal information as defined in Section 5 [815 ILCS 530/5] in paragraph (1) of the definition of “personal information”:

(A)the toll-free numbers and addresses for consumer reporting agencies;

(B)the toll-free number, address, and website address for the Federal Trade Commission; and

(C)a statement that the individual can obtain information from these sources about fraud alerts and security freezes.

(2)With respect to personal information defined in Section 5 in paragraph (2) of the definition of “personal information”, notice may be provided in electronic or other form directing the Illinois resident whose personal information has been breached to promptly change his or her user name or password and security question or answer, as applicable, or to take other steps appropriate to protect all online accounts for which the resident uses the same user name or email address and password or security question and answer.

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

(b)Any data collector that maintains or stores, but does not own or license, computerized data that includes personal information that the data collector does not own or license shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person. In addition to providing such notification to the owner or licensee, the data collector shall cooperate with the owner or licensee in matters relating to the breach. That cooperation shall include, but need not be limited to, (i) informing the owner or licensee of the breach, including giving notice of the date or approximate date of the breach and the nature of the breach, and (ii) informing the owner or licensee of any steps the data collector has taken or plans to take relating to the breach. The data collector's cooperation shall not, however, be deemed to require either the disclosure of confidential business information or trade secrets or the notification of an Illinois resident who may have been affected by the breach.

(b-5)The notification to an Illinois resident required by subsection (a) of this Section may be delayed if an appropriate law enforcement agency determines that notification will interfere with a criminal investigation and provides the data collector with a written request for the delay. However, the data collector must notify the Illinois resident as soon as notification will no longer interfere with the investigation.

(c) For purposes of this Section, notice to consumers may be provided by one of the following methods:

(1) written notice;

(2) electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures for notices legally required to be in writing as set forth in Section 7001 of Title 15 of the United States Code; or

(3) substitute notice, if the data collector demonstrates that the cost of providing notice would exceed \$250,000 or that the affected class of subject persons to be notified exceeds 500,000, or the data collector does not have sufficient contact information. Substitute notice shall consist of all of the following: (i) email notice if the data collector has an email address for the subject persons; (ii) conspicuous posting of the notice on the data collector's web site page if the data collector maintains one; and (iii) notification to major statewide media or, if the breach impacts residents in one geographic area, to prominent local media in areas where affected individuals are likely to reside if such notice is reasonably calculated to give actual notice to persons whom notice is required.

(d) Notwithstanding any other subsection in this Section, a data collector that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this Act, shall be deemed in compliance with the notification requirements of this Section if the data collector notifies subject persons in accordance with its policies in the event of a breach of the security of the system data.

(e)

(1) This subsection does not apply to data collectors that are covered entities or business associates and are in compliance with Section 50 [815 ILCS 530/50].

(2) Any data collector required to issue notice pursuant to this Section to more than 500 Illinois residents as a result of a single breach of the security system shall provide notice to the Attorney General of the breach, including:

(A) A description of the nature of the breach of security or unauthorized acquisition or use.

(B) The number of Illinois residents affected by such incident at the time of notification.

(C) Any steps the data collector has taken or plans to take relating to the incident.

Such notification must be made in the most expedient time possible and without unreasonable delay but in no event later than when the data collector provides notice to consumers pursuant to this Section. If the date of the breach is unknown at the time the notice is sent to the Attorney General, the data collector shall send the Attorney General the date of the breach as soon as possible.

Upon receiving notification from a data collector of a breach of personal information, the Attorney General may publish the name of the data collector that suffered the breach, the types of personal information compromised in the breach, and the date range of the breach.

History

[P.A. 94-36](#), § 10; [94-947](#), § 5; [97-483](#), § 5; [99-503](#), § 5; [99-503](#), § 5; 2017 [P.A. 100-201](#), § 800, effective August 18, 2017; 2019 [P.A. 101-343](#), § 5, effective January 1, 2020.

Annotations

Notes

Amendment Notes

The 2006 amendment by P.A. 94-947, effective June 27, 2006, added “at no charge” in (a); and added (b-5).

The 2011 amendment by P.A. 97-483, effective January 1, 2012, added the last two sentences to (a); in (b), inserted “or stores, but does not own or license” in the first sentence and added the last three sentences; inserted “to an Illinois resident” in the first sentence of (b-5); and substituted “any other subsection in this Section” and “subsection (c)” in (d).

The 2016 amendment by P.A. 99-503, effective January 1, 2017, added “information as follows” to the end of the last sentence of the introductory language of (a); added (a)(1) and (a)(2); redesignated former (a)(i) through (a)(iii) as (a)(1)(A) through (a)(1)(C); added “or, if the breach impacts residents in one geographic area, to prominent local media in areas where affected individuals are likely to reside if such notice is reasonably calculated to give actual notice to persons whom notice is required” to the end (c)(3)(iii); and made stylistic changes.

The 2017 amendment by P.A. 100-201, effective Aug. 18, 2017, redesignated the former second paragraph of (a)(1) as the second paragraph of (a)(2).

The 2019 amendment by P.A. 101-343, effective January 1, 2020, added “notice to Attorney General” in the section heading; and added (e).

CASE NOTES

Construction

Duty

Relief

Standing

Construction

Statute as a whole treats an “owner or licensee” differently from an “Illinois resident” in connection with disclosure obligations. [*Worix v. MedAssets, Inc.*, 869 F. Supp. 2d 893, 2012 U.S. Dist. LEXIS 56773 \(N.D. Ill. 2012\)](#).

Duty

Where an employee’s computer hard drive containing personal information was stolen, a patient’s negligence claim failed because the patient could not rely on Illinois’ Personal Information Protection Act to establish the company’s duty to inform the patient of the theft since the patient was not the “owner or licensee” of the information that the company held and the company did not owe the patient a duty of prompt disclosure under [*815 ILCS 530/10\(b\)*](#). [*Worix v. MedAssets, Inc.*, 869 F. Supp. 2d 893, 2012 U.S. Dist. LEXIS 56773 \(N.D. Ill. 2012\)](#).

Relief

Former employees who personal information was disclosed to each other after the Board had the printing company print and mail an insurance benefit plan enrollment list to the former employees were correct in arguing that the Board violated the Personal Information Protection Act because the Board was an [815 ILCS 530/5](#) data collector that disclosed the personal information regarding those former employees. However, the former employees could not show that the violation could lead to a remedy, as the Board complied with [815 ILCS 530/10\(b\)](#) disclosed the security breach to the former employees in a letter that asked them to return or destroy the list, which was the statutory remedy prescribed. [Cooney v. Chi. Pub. Schs., 407 Ill. App. 3d 358, 347 Ill. Dec. 733, 943 N.E.2d 23, 2010 Ill. App. LEXIS 1424 \(Ill. App. Ct. 1st Dist. 2010\).](#)

Standing

As a nonresident consumer, plaintiff had no cause of action against defendants under 15 ILCS 530/10(b) of the Illinois Personal Information Protection Act. [Irwin v. Jimmy John's Franchise, LLC, 175 F. Supp. 3d 1064, 2016 U.S. Dist. LEXIS 48162 \(C.D. Ill. 2016\).](#)

Courts properly dismissed the claims because the patients did not have standing to bring their claims when their allegations of injury were clearly speculative. [Maglio v. Advocate Health & Hosps. Corp., 2015 IL App \(2d\) 140782, 396 Ill. Dec. 861, 40 N.E.3d 746, 2015 Ill. App. LEXIS 596 \(Ill. App. Ct. 2d Dist. 2015\).](#)

Illinois Compiled Statutes Annotated
Copyright © 2020 Matthew Bender & Company, Inc.
member of the LexisNexis Group. All rights reserved.

End of Document

35-A M.R.S. § 9301

Current with the Second Regular Session of the 129th Maine Legislature.

Maine Revised Statutes Annotated by LexisNexis® > Title 35-A. Public Utilities (Pts. 1 — 8) > Part 7. Telecommunications (Chs. 71 — 94) > Chapter 94. Broadband Internet Access Service Customer Privacy (§ 9301)

§ 9301. Privacy of broadband Internet access service customer personal information

1. Definitions. As used in this section, unless the context otherwise indicates, the following terms have the following meanings.

A.“Broadband Internet access service” means a mass-market retail service by wire or radio that provides the capability to transmit data to and receive data from all or substantially all Internet endpoints, including any capabilities that are incidental to and enable the operation of the service, excluding dial-up Internet access service.

B.“Customer” means an applicant for or a current or former subscriber of broadband Internet access service.

C.“Customer personal information” means:

(1)Personally identifying information about a customer, including but not limited to the customer’s name, billing information, social security number, billing address and demographic data; and

(2)Information from a customer’s use of broadband Internet access service, including but not limited to:

(a)The customer’s web browsing history;

(b)The customer’s application usage history;

(c)The customer’s precise geolocation information;

(d)The customer’s financial information;

(e)The customer’s health information;

(f)Information pertaining to the customer’s children;

(g)The customer’s device identifier, such as a media access control address, international mobile equipment identity or Internet protocol address;

(h)The content of the customer’s communications; and

(i)The origin and destination Internet protocol addresses.

D.“Provider” means a person who provides broadband Internet access service.

2. Privacy of customer personal information. A provider may not use, disclose, sell or permit access to customer personal information, except as provided in subsections 3 and 4, Title 16, chapter 3, subchapters 10 and 11 and 18 United States Code, Section 2703.

3. Customer consent exception. Consent of a customer is governed by this subsection.

35-A M.R.S. § 9301

A. A provider may use, disclose, sell or permit access to a customer's customer personal information if the customer gives the provider express, affirmative consent to such use, disclosure, sale or access. A customer may revoke the customer's consent under this paragraph at any time.

B. A provider may not:

- (1) Refuse to serve a customer who does not provide consent under paragraph A; or
- (2) Charge a customer a penalty or offer a customer a discount based on the customer's decision to provide or not provide consent under paragraph A.

C. A provider may use, disclose, sell or permit access to information the provider collects pertaining to a customer that is not customer personal information, except upon written notice from the customer notifying the provider that the customer does not permit the provider to use, disclose, sell or permit access to that information.

4. Other exceptions. Notwithstanding the provisions of subsections 2 and 3, a provider may collect, retain, use, disclose, sell and permit access to customer personal information without customer approval:

- A.** For the purpose of providing the service from which such information is derived or for the services necessary to the provision of such service;
- B.** To advertise or market the provider's communications-related services to the customer;
- C.** To comply with a lawful court order;
- D.** To initiate, render, bill for and collect payment for broadband Internet access service;
- E.** To protect users of the provider's or other providers' services from fraudulent, abusive or unlawful use of or subscription to such services; and
- F.** To provide geolocation information concerning the customer:
 - (1) For the purpose of responding to a customer's call for emergency services, to a public safety answering point; a provider of emergency medical or emergency dispatch services; a public safety, fire service or law enforcement official; or a hospital emergency or trauma care facility; or
 - (2) To a provider of information or database management services solely for the purpose of assisting in the delivery of emergency services in response to an emergency.

5. Security of customer personal information. A provider shall take reasonable measures to protect customer personal information from unauthorized use, disclosure or access.

A. In implementing security measures required by this subsection, a provider shall take into account each of the following factors:

- (1) The nature and scope of the provider's activities;
- (2) The sensitivity of the data the provider collects;
- (3) The size of the provider; and
- (4) The technical feasibility of the security measures.

B. A provider may employ any lawful measure that allows the provider to comply with the requirements of this subsection.

6. Notice required. A provider shall provide to each of the provider's customers a clear, conspicuous and nondeceptive notice at the point of sale and on the provider's publicly accessible website of the provider's obligations and a customer's rights under this section.

7. Applicability. The requirements of this section apply to providers operating within the State when providing broadband Internet access service to customers that are physically located and billed for service received in the State.

History

[2019 ch. 216](#), § 1, effective July 1, 2020.

Maine Revised Statutes Annotated by LexisNexis®
Copyright © 2020 All rights reserved.

End of Document

MCLS Ch. 500, Act 218, Ch. 5A

This document is current through Public Act 1-192 from the 2020 Legislative Session

**Michigan Compiled Laws Service > Chapter 500 Insurance Code of 1956 (§§ 500.100 — 500.8302)
> Act 218 of 1956 (Chs. 1 — 83) > Chapter 5A Data Security [Effective January 20, 2021] (§§
500.550 — 500.565)**

Chapter 5A Data Security [Effective January 20, 2021]

History

[*Pub Acts 2018, No. 690*](#), effective January 20, 2021.

Michigan Compiled Laws Service
Copyright © 2020 Matthew Bender & Company, Inc.
a member of the LexisNexis Group. All rights reserved.

End of Document

MCLS § 500.550

This document is current through Public Act 1-192 from the 2020 Legislative Session

**Michigan Compiled Laws Service > Chapter 500 Insurance Code of 1956 (§§ 500.100 — 500.8302)
> Act 218 of 1956 (Chs. 1 — 83) > Chapter 5A Data Security [Effective January 20, 2021] (§§
500.550 — 500.565)**

§ 500.550. Private cause of action not created; standards. [Effective January 20, 2021]

Sec. 550.

This chapter does not create or imply a private cause of action for violation of its provisions and does not curtail a private cause of action that would otherwise exist in the absence of this chapter. Notwithstanding any other provision of law, this chapter establishes the exclusive standards, for this state, applicable to licensees for data security, the investigation of a cybersecurity event, and notification to the director.

History

[Pub Acts 2018, No. 690](#), effective January 20, 2021.

Michigan Compiled Laws Service
Copyright © 2020 Matthew Bender & Company, Inc.
a member of the LexisNexis Group. All rights reserved.

End of Document

MCLS § 500.553

This document is current through Public Act 1-192 from the 2020 Legislative Session

**Michigan Compiled Laws Service > Chapter 500 Insurance Code of 1956 (§§ 500.100 — 500.8302)
> Act 218 of 1956 (Chs. 1 — 83) > Chapter 5A Data Security [Effective January 20, 2021] (§§
500.550 — 500.565)**

§ 500.553. Definitions. [Effective January 20, 2021]

Sec. 553.

As used in this chapter:

(a)“Authorized individual” means an individual known to and screened by the licensee and determined to be necessary and appropriate to have access to the nonpublic information held by the licensee and its information systems.

(b)“Consumer” means an individual, including, but not limited to, an applicant, a policyholder, an insured, a beneficiary, a claimant, and a certificate holder, who is a resident of this state and whose nonpublic information is in a licensee’s possession, custody, or control.

(c)“Cybersecurity event” means an event that results in unauthorized access to and acquisition of, or disruption or misuse of, an information system or nonpublic information stored on an information system. Cybersecurity event does not include either of the following:

(i)The unauthorized acquisition of encrypted nonpublic information if the encryption, process, or key is not also acquired, released, or used without authorization.

(ii)The unauthorized access to data by a person if the access meets both of the following criteria:

(A)The person acted in good faith in accessing the data.

(B)The access was related to activities of the person.

(d)“Encrypted” means the transformation of data into a form that results in a low probability of assigning meaning without the use of a protective process or key.

(e)“Information security program” means the administrative, technical, and physical safeguards that a licensee uses to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle nonpublic information.

(f)“Information system” means a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of electronic nonpublic information, as well as any specialized system such as an industrial or process controls system, a telephone switching and private branch exchange system, or an environmental control system.

(g)“Licensee” means a licensed insurer or producer, and other persons licensed or required to be licensed, authorized, or registered, or holding or required to hold a certificate of authority under this act. Licensee does not include a purchasing group or a risk retention group chartered and licensed in a state other than this state or a person that is acting as an assuming insurer that is domiciled in another state or jurisdiction.

(h)“Multi-factor authentication” means authentication through verification of at least 2 of the following types of authentication factors:

(i)Knowledge factors, such as a password.

MCLS § 500.553

(ii) Possession factors, such as a token or text message on a mobile phone.

(iii) Inherence factors, such as a biometric characteristic.

(i) “Nonpublic information” means electronic information that is not publicly available information and is any of the following:

(i) Business-related information of a licensee, the tampering with which, or unauthorized disclosure, access, or use of which, would cause a material adverse impact to the business, operations, or security of the licensee.

(ii) Any information concerning a consumer that because of name, number, personal mark, or other identifier can be used to identify the consumer, in combination with any 1 or more of the following data elements:

(A) Social Security number.

(B) Driver license number or nondriver identification card number.

(C) Financial account number, or credit or debit card number.

(D) Any security code, access code, or password that would permit access to a consumer’s financial account.

(E) Biometric records.

(iii) Any information or data, except age or gender, in any form or medium created by or derived from a health care provider or a consumer, that can be used to identify a particular consumer, and that relates to any of the following:

(A) The past, present, or future physical, mental, or behavioral health or condition of any consumer or a member of the consumer’s family.

(B) The provision of health care to any consumer.

(C) Payment for the provision of health care to any consumer.

(j) “Publicly available information” means any information that a licensee has a reasonable basis to believe is lawfully made available to the general public from federal, state, or local government records, by widely distributed media, or by disclosures to the general public that are required to be made by federal, state, or local law. A licensee has a reasonable basis to believe that information is lawfully made available to the general public if both of the following apply:

(i) The licensee has taken steps to determine that the information is of the type that is available to the general public.

(ii) If an individual can direct that the information not be made available to the general public, that the licensee’s consumer has not directed that the information not be made available to the general public.

(k) “Risk assessment” means the risk assessment that each licensee is required to conduct under section 555(3).

(l) “Third-party service provider” means a person that is not a licensee and that contracts with a licensee to maintain, process, or store, or otherwise is permitted access to nonpublic information, through its provision of services to the licensee.

History

MCLS § 500.553

Michigan Compiled Laws Service
Copyright © 2020 Matthew Bender & Company, Inc.
a member of the LexisNexis Group. All rights reserved.

End of Document

MCLS § 500.555

This document is current through Public Act 1-192 from the 2020 Legislative Session

**Michigan Compiled Laws Service > Chapter 500 Insurance Code of 1956 (§§ 500.100 — 500.8302)
> Act 218 of 1956 (Chs. 1 — 83) > Chapter 5A Data Security [Effective January 20, 2021] (§§
500.550 — 500.565)**

§ 500.555. Comprehensive written information security program. [Effective January 20, 2021]

Sec. 555.

(1) Commensurate with the size and complexity of the licensee, the nature and scope of the licensee's activities, including its use of third-party service providers, and the sensitivity of the nonpublic information used by the licensee or in the licensee's possession, custody, or control, each licensee shall develop, implement, and maintain a comprehensive written information security program, based on the licensee's risk assessment, that contains administrative, technical, and physical safeguards for the protection of nonpublic information and the licensee's information system.

(2) A licensee's information security program must be designed to do all of the following:

- (a)** Protect the security and confidentiality of nonpublic information and the security of the information system.
- (b)** Protect against any threats or hazards to the security or integrity of nonpublic information and the information system.
- (c)** Protect against unauthorized access to or use of nonpublic information, and minimize the likelihood of harm to any consumer.
- (d)** Maintain policies and procedures for the secure disposal on a periodic basis of any nonpublic information that is no longer necessary for business operations or for other legitimate business purposes.

(3) A licensee shall do all of the following:

- (a)** Designate 1 or more employees, an affiliate, or an outside vendor to act on behalf of the licensee that is responsible for the information security program.
- (b)** Identify reasonably foreseeable internal or external threats that could result in unauthorized access, transmission, disclosure, misuse, alteration, or destruction of nonpublic information, including the security of information systems and nonpublic information that are accessible to, or held by, third-party service providers.
- (c)** Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of the nonpublic information.
- (d)** Assess the sufficiency of policies, procedures, information systems, and other safeguards in place to manage these threats, including consideration of threats in each relevant area of the licensee's operations, including all of the following:
 - (i)** Employee training and management.
 - (ii)** Information systems, including network and software design, as well as information classification, governance, processing, storage, transmission, and disposal.

(iii)Detecting, preventing, and responding to attacks, intrusions, or other systems failures.

(e) Implement information safeguards to manage the threats identified in its ongoing assessment, and, no less than annually, assess the effectiveness of the safeguards' key controls, systems, and procedures.

(4)Based on its risk assessment, a licensee shall do all of the following:

(a) Design its information security program to mitigate the identified risks, commensurate with the size and complexity of the licensee, the nature and scope of the licensee's activities, including its use of third-party service providers, and the sensitivity of the nonpublic information used by the licensee or in the licensee's possession, custody, or control.

(b)Determine which of the following security measures are appropriate and implement those appropriate security measures:

(i) Placing access controls on information systems, including controls to authenticate and permit access only to authorized individuals to protect against the unauthorized acquisition of nonpublic information.

(ii) Identifying and managing the data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes in accordance with their relative importance to business objectives and the organization's risk strategy.

(iii) Restricting physical access to nonpublic information to authorized individuals only.

(iv) Protecting by encryption or other appropriate means all nonpublic information while being transmitted over an external network and all nonpublic information stored on a laptop computer or other portable computing or storage device or media.

(v) Adopting secure development practices for in-house developed applications utilized by the licensee.

(vi) Adding procedures for evaluating, assessing, or testing the security of externally developed applications used by the licensee.

(vii) Modifying the information system in accordance with the licensee's information security program.

(viii) Using effective controls, which may include multi-factor authentication procedures for employees accessing nonpublic information.

(ix) Regularly testing and monitoring systems and procedures to detect actual and attempted attacks on, or intrusions into, information systems.

(x) Including audit trails within the information security program designed to detect and respond to cybersecurity events and designed to reconstruct material financial transactions sufficient to support normal operations and obligations of the licensee.

(xi) Implementing measures to protect against destruction, loss, or damage of nonpublic information due to environmental hazards, such as fire and water damage or other catastrophes or technological failures.

(xii) Developing, implementing, and maintaining procedures for the secure disposal of nonpublic information in any format.

(c) Include cybersecurity risks in the licensee's enterprise risk management process.

(d) Stay informed regarding emerging threats or vulnerabilities and utilize reasonable security measures when sharing information relative to the character of the sharing and the type of information shared.

(e) Provide its personnel with cybersecurity awareness training that is updated as necessary to reflect risks identified by the licensee in the risk assessment.

MCLS § 500.555

(5) If a licensee has a board of directors, the board or an appropriate committee of the board shall, at a minimum, do all of the following:

(a) Require the licensee's executive management or its delegates to develop, implement, and maintain the licensee's information security program.

(b) Require the licensee's executive management or its delegates to report in writing, at least annually, all of the following information:

(i) The overall status of the information security program and the licensee's compliance with this chapter.

(ii) Material matters related to the information security program, addressing issues such as risk assessment, risk management and control decisions, results of testing, cybersecurity events or violations, and management's responses to the material matters described in this subparagraph, and recommendations for changes in the information security program.

(iii) If executive management delegates any of its responsibilities under this section, it shall oversee the development, implementation, and maintenance of the licensee's information security program prepared by a delegate and shall receive a report from the delegate complying with the requirements of the report to the board of directors.

(6) A licensee shall exercise due diligence in selecting its third-party service provider. A licensee shall require a third-party service provider to implement appropriate administrative, technical, and physical measures to protect and secure the information systems and nonpublic information that are accessible to, or held by, the third-party service provider.

(7) A licensee shall monitor, evaluate, and adjust, as appropriate, the information security program consistent with any relevant changes in technology, the sensitivity of its nonpublic information, internal or external threats to information, and the licensee's own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements, and changes to information systems.

(8) As part of its information security program, each licensee shall establish a written incident response plan designed to promptly respond to, and recover from, any cybersecurity event that compromises the confidentiality, integrity, or availability of nonpublic information in its possession, the licensee's information systems, or the continuing functionality of any aspect of the licensee's business or operations. An incident response plan under this subsection must address all of the following areas:

(a) The internal process for responding to a cybersecurity event.

(b) The goals of the incident response plan.

(c) The definition of clear roles, responsibilities, and levels of decision-making authority.

(d) External and internal communications and information sharing.

(e) Identification of requirements for the remediation of any identified weaknesses in information systems and associated controls.

(f) Documentation and reporting regarding cybersecurity events and related incident response activities.

(g) The evaluation and revision as necessary of the incident response plan following a cybersecurity event.

(9) By February 15 of each year, each insurer domiciled in this state shall submit to the director a written statement, certifying that the insurer is in compliance with the requirements of this section. Each insurer shall maintain for examination by the department all records, schedules, and data supporting this certificate for 5 years. To the extent an insurer has identified areas, systems, or processes that require material improvement, updating, or redesign, the insurer shall document the identification and the remedial efforts planned and underway to address the areas, systems, or processes. The documentation described in this subsection must be available for inspection by the director.

History

[*Pub Acts 2018, No. 690*](#), effective January 20, 2021.

Michigan Compiled Laws Service
Copyright © 2020 Matthew Bender & Company, Inc.
a member of the LexisNexis Group. All rights reserved.

End of Document

MCLS § 500.557

This document is current through Public Act 1-192 from the 2020 Legislative Session

**Michigan Compiled Laws Service > Chapter 500 Insurance Code of 1956 (§§ 500.100 — 500.8302)
> Act 218 of 1956 (Chs. 1 — 83) > Chapter 5A Data Security [Effective January 20, 2021] (§§
500.550 — 500.565)**

§ 500.557. Investigation of cybersecurity event. [Effective January 20, 2021]

Sec. 557.

(1) If the licensee learns that a cybersecurity event has or may have occurred, the licensee or an outside vendor or service provider, or both, designated to act on behalf of the licensee, shall conduct a prompt investigation.

(2) During the investigation under subsection (1), the licensee, or an outside vendor or service provider, or both, designated to act on behalf of the licensee, shall, at a minimum, do as much of the following as possible:

(a) Determine whether a cybersecurity event has occurred.

(b) Assess the nature and scope of the cybersecurity event.

(c) Identify any nonpublic information that may have been involved in the cybersecurity event.

(d) Perform or oversee reasonable measures to restore the security of the information systems compromised in the cybersecurity event to prevent further unauthorized acquisition, release, or use of nonpublic information in the licensee's possession, custody, or control.

(3) The licensee shall maintain records concerning all cybersecurity events for at least 5 years from the date of the cybersecurity event and shall produce those records on demand of the director.

History

[Pub Acts 2018, No. 690](#), effective January 20, 2021.

Michigan Compiled Laws Service
Copyright © 2020 Matthew Bender & Company, Inc.
a member of the LexisNexis Group. All rights reserved.

End of Document

MCLS § 500.559

This document is current through Public Act 1-192 from the 2020 Legislative Session

**Michigan Compiled Laws Service > Chapter 500 Insurance Code of 1956 (§§ 500.100 — 500.8302)
> Act 218 of 1956 (Chs. 1 — 83) > Chapter 5A Data Security [Effective January 20, 2021] (§§
500.550 — 500.565)**

§ 500.559. Cybersecurity event involving nonpublic information; notice to director. [Effective January 20, 2021]

Sec. 559.

(1)Each licensee shall notify the director as promptly as possible but not later than 10 business days after a determination that a cybersecurity event involving nonpublic information that is in the possession of a licensee has occurred when either of the following criteria has been met:

(a)This state is the licensee's state of domicile, for an insurer, or this state is the licensee's home state, for an insurance producer as that term is defined in section 1201, and the cybersecurity event has a reasonable likelihood of materially harming either of the following:

(i)A consumer residing in this state.

(ii)Any material part of a normal operation of the licensee.

(b)The licensee reasonably believes that the nonpublic information involved is of 250 or more consumers residing in this state and is either of the following:

(i)A cybersecurity event impacting the licensee of which notice is required to be provided to any government body, self-regulatory agency, or other supervisory body under any state or federal law.

(ii)A cybersecurity event that has a reasonable likelihood of materially harming either of the following:

(A)Any consumer residing in this state.

(B)Any material part of the normal operation of the licensee.

(2)The licensee shall provide the information under this subsection in electronic form as directed by the director. The licensee has a continuing obligation to update and supplement initial and subsequent notifications to the director regarding material changes to previously provided information relating to the cybersecurity event. The licensee shall provide as much of the following information as possible:

(a)The date of the cybersecurity event.

(b)A description of how the information was exposed, lost, stolen, or breached, including the specific roles and responsibilities of third-party service providers, if any.

(c)How the cybersecurity event was discovered.

(d)Whether any lost, stolen, or breached information has been recovered and, if so, how this was done.

(e)The identity of the source of the cybersecurity event.

(f)Whether the licensee has filed a police report or has notified any regulatory, government, or law enforcement agencies and, if so, when the notification was provided.

MCLS § 500.559

- (g)**A description of the specific types of information acquired without authorization. As used in this subdivision, “specific types of information” means particular data elements including, for example, types of medical information, types of financial information, or types of information allowing identification of the consumer.
- (h)**The period during which the information system was compromised by the cybersecurity event.
- (i)**The number of total consumers in this state affected by the cybersecurity event. The licensee shall provide the best estimate in the initial report to the director and update this estimate with each subsequent report to the director under this section.
- (j)**The results of any internal review identifying a lapse in either automated controls or internal procedures, or confirming that all automated controls or internal procedures were followed.
- (k)**A description of efforts being undertaken to remediate the situation that permitted the cybersecurity event to occur.
- (l)**A copy of the licensee’s privacy policy and a statement outlining the steps the licensee will take to investigate and notify consumers affected by the cybersecurity event.
- (m)**The name of a contact person who is both familiar with the cybersecurity event and authorized to act for the licensee.
- (3)**A licensee shall comply with this chapter, as applicable, and provide a copy of the notice sent to consumers under this chapter, if a licensee is required to notify the director under section 559.
- (4)**For a cybersecurity event in a system maintained by a third-party service provider, of which the licensee has become aware, the licensee shall treat the event as it would under this section. The computation of the licensee’s deadlines begins on the day after the third-party service provider notifies the licensee of the cybersecurity event or the licensee otherwise has actual knowledge of the cybersecurity event, whichever is earlier. This chapter does not prevent or abrogate an agreement between a licensee and another licensee, a third-party service provider, or any other party to fulfill any of the investigation requirements imposed under section 557 or notice requirements imposed under this section.
- (5)**For a cybersecurity event involving nonpublic information that is used by the licensee that is acting as an assuming insurer or in the possession, custody, or control of a licensee that is acting as an assuming insurer and that does not have a direct contractual relationship with the affected consumers, the assuming insurer shall notify its affected ceding insurers and the director of its state of domicile within 10 business days after making the determination that a cybersecurity event has occurred. The ceding insurers that have a direct contractual relationship with affected consumers shall fulfill the consumer notification requirements imposed under this section. For a cybersecurity event involving nonpublic information that is in the possession, custody, or control of a third-party service provider of a licensee that is an assuming insurer, the assuming insurer shall notify its affected ceding insurers and the director of its state of domicile within 10 business days after receiving notice from its third-party service provider that a cybersecurity event has occurred. The ceding insurers that have a direct contractual relationship with affected consumers shall fulfill the consumer notification requirements imposed under this chapter.
- (6)**A licensee acting as an assuming insurer does not have other notice obligations relating to a cybersecurity event or other data breach under this section or any other law of this state.
- (7)**For a cybersecurity event involving nonpublic information that is in the possession, custody, or control of a licensee that is an insurer or its third-party service provider for which a consumer accessed the insurer’s services through an independent insurance producer, and for which consumer notice is required under this chapter, the insurer shall notify the producers of record of all affected consumers of the cybersecurity event not later than the time at which notice is provided to the affected consumers. The insurer is excused from this obligation for any producer who is not authorized by law or contract to sell, solicit, or negotiate on behalf of the insurer, and in those instances in which the insurer does not have the current producer of record information for any individual consumer.

History

[*Pub Acts 2018, No. 690*](#), effective January 20, 2021.

Michigan Compiled Laws Service
Copyright © 2020 Matthew Bender & Company, Inc.
a member of the LexisNexis Group. All rights reserved.

End of Document

MCLS § 500.561

This document is current through Public Act 1-192 from the 2020 Legislative Session

**Michigan Compiled Laws Service > Chapter 500 Insurance Code of 1956 (§§ 500.100 — 500.8302)
> Act 218 of 1956 (Chs. 1 — 83) > Chapter 5A Data Security [Effective January 20, 2021] (§§
500.550 — 500.565)**

§ 500.561. Notice of cybersecurity event to residents of state. [Effective January 20, 2021]

Sec. 561.

(1) Unless the licensee determines that the cybersecurity event has not or is not likely to cause substantial loss or injury to, or result in identity theft with respect to, 1 or more residents of this state, a licensee that owns or licenses data that are included in a database that discovers a cybersecurity event, or receives notice of a cybersecurity event under subsection (2), shall provide a notice of the cybersecurity event to each resident of this state who meets 1 or more of the following:

(a) That resident's unencrypted and unredacted personal information was accessed and acquired by an unauthorized person.

(b) That resident's personal information was accessed and acquired in encrypted form by a licensee with unauthorized access to the encryption key.

(2) Unless the licensee determines that the cybersecurity event has not or is not likely to cause substantial loss or injury to, or result in identity theft with respect to, 1 or more residents of this state, a licensee that maintains a database that includes data that the licensee does not own or license that discovers a breach of the security of the database shall provide a notice to the owner or licensor of the information of the cybersecurity event.

(3) In determining whether a cybersecurity event is not likely to cause substantial loss or injury to, or result in identity theft with respect to, 1 or more residents of this state under subsection (1) or (2), a licensee shall act with the care an ordinarily prudent person or agency in like position would exercise under similar circumstances.

(4) A licensee shall provide any notice required under this section without unreasonable delay. A licensee may delay providing notice without violating this subsection if either of the following is met:

(a) A delay is necessary in order for the licensee to take any measures necessary to determine the scope of the cybersecurity event and restore the reasonable integrity of the database. However, the licensee shall provide the notice required under this subsection without unreasonable delay after the licensee completes the measures necessary to determine the scope of the cybersecurity event and restore the reasonable integrity of the database.

(b) A law enforcement agency determines and advises the licensee that providing a notice will impede a criminal or civil investigation or jeopardize homeland or national security. However, the licensee shall provide the notice required under this section without unreasonable delay after the law enforcement agency determines that providing the notice will no longer impede the investigation or jeopardize homeland or national security.

(5) A licensee shall provide any notice required under this section by providing 1 or more of the following to the recipient:

(a) Written notice sent to the recipient at the recipient's postal address in the records of the licensee.

MCLS § 500.561

(b)Written notice sent electronically to the recipient if any of the following are met:

- (i)**The recipient has expressly consented to receive electronic notice.
- (ii)**The licensee has an existing business relationship with the recipient that includes periodic electronic mail communications and based on those communications the licensee reasonably believes that it has the recipient's current electronic mail address.
- (iii)**The licensee conducts its business primarily through internet account transactions or on the internet.

(c)If not otherwise prohibited by state or federal law, notice given by telephone by an individual who represents the licensee if all of the following are met:

- (i)**The notice is not given in whole or in part by use of a recorded message.
- (ii)**The recipient has expressly consented to receive notice by telephone, or if the recipient has not expressly consented to receive notice by telephone, the licensee also provides notice under subdivision (a) or (b) if the notice by telephone does not result in a live conversation between the individual representing the licensee and the recipient within 3 business days after the initial attempt to provide telephonic notice.

(d)Substitute notice, if the licensee demonstrates that the cost of providing notice under subdivision (a), (b), or (c) will exceed \$250,000.00 or that the licensee has to provide notice to more than 500,000 residents of this state. A licensee provides substitute notice under this subdivision by doing all of the following:

- (i)**If the licensee has electronic mail addresses for any of the residents of this state who are entitled to receive the notice, providing electronic notice to those residents.
- (ii)**If the licensee maintains a website, conspicuously posting the notice on that website.
- (iii)**Notifying major statewide media. A notification under this subparagraph must include a telephone number or a website address that a person may use to obtain additional assistance and information.

(6)A notice under this section must do all of the following:

- (a)**For a notice provided under subsection (5)(a) or (b), be written in a clear and conspicuous manner and contain the content required under subdivisions (c) to (g).
- (b)**For a notice provided under subsection (5)(c), clearly communicate the content required under subdivisions (c) to (g) to the recipient of the telephone call.
- (c)**Describe the cybersecurity event in general terms.
- (d)**Describe the type of personal information that is the subject of the unauthorized access or use.
- (e)**If applicable, generally describe what the licensee providing the notice has done to protect data from further security breaches.
- (f)**Include a telephone number where a notice recipient may obtain assistance or additional information.
- (g)**Remind notice recipients of the need to remain vigilant for incidents of fraud and identity theft.

(7)A licensee may provide any notice required under this section under an agreement between the licensee and another licensee, if the notice provided under the agreement does not conflict with this section.

(8)Except as provided in this subsection, after a licensee provides a notice under this section, the licensee shall notify each consumer reporting agency that compiles and maintains files on consumers on a nationwide basis, as defined in [15 USC 1681a\(p\)](#), of the cybersecurity event without unreasonable delay. A notification under this subsection must include the number of notices that the licensee provided to residents of this state and the timing of those notices. This subsection does not apply if either of the following is met:

MCLS § 500.561

(a) The licensee is required under this section to provide notice of a cybersecurity event to 1,000 or fewer residents of this state.

(b) The licensee is subject to [15 USC 6801](#) to [6809](#).

(9) A licensee that is subject to and complies with the health insurance portability and accountability act of 1996, *Public Law 104-191*, and with regulations promulgated under that act, 45 CFR parts 160 and 164, for the prevention of unauthorized access to customer information and customer notice is considered to be in compliance with this section.

(10) A person that provides notice of a cybersecurity event in the manner described in this section when a cybersecurity event has not occurred, with the intent to defraud, is guilty of a misdemeanor punishable as follows:

(a) Except as otherwise provided under subdivisions (b) and (c), by imprisonment for not more than 93 days or a fine of not more than \$250.00 for each violation, or both.

(b) For a second violation, by imprisonment for not more than 93 days or a fine of not more than \$500.00 for each violation, or both.

(c) For a third or subsequent violation, by imprisonment for not more than 93 days or a fine of not more than \$750.00 for each violation, or both.

(11) Subject to subsection (12), a person that knowingly fails to provide a notice of a cybersecurity event required under this section may be ordered to pay a civil fine of not more than \$250.00 for each failure to provide notice. The attorney general or a prosecuting attorney may bring an action to recover a civil fine under this section.

(12) The aggregate liability of a person for civil fines under subsection (11) for multiple violations of subsection (11) that arise from the same cybersecurity event must not exceed \$750,000.00.

(13) Subsections (10) and (11) do not affect the availability of any civil remedy for a violation of state or federal law.

(14) This section applies to the discovery or notification of a breach of the security of a database that occurs after December 31, 2019.

(15) This section does not apply to the access or acquisition by a person or agency of federal, state, or local government records or documents lawfully made available to the general public.

(16) This section deals with subject matter that is of statewide concern, and any charter, ordinance, resolution, regulation, rule, or other action by a municipal corporation or other political subdivision of this state to regulate, directly or indirectly, any matter expressly set forth in this section is preempted.

(17) As used in this section:

(a) "Data" means computerized information.

(b) "Identity theft" means a person doing any of the following:

(i) With intent to defraud or violate the law, using or attempting to use the personal information of another person to do either of the following:

(A) Obtain credit, goods, services, money, property, a vital record, a confidential telephone record, medical records or information, or employment.

(B) Commit another unlawful act.

(ii) By concealing, withholding, or misrepresenting the person's identity, using or attempting to use the personal information of another person to do either of the following:

(A) Obtain credit, goods, services, money, property, a vital record, a confidential telephone record, medical records or information, or employment.

MCLS § 500.561

(B)Commit another unlawful act.

(c)“Personal information” means the first name or first initial and last name linked to 1 or more of the following data elements of a resident of this state:

(i)A Social Security number.

(ii)A driver license number or state personal identification card number.

(iii)A demand deposit or other financial account number, or credit card or debit card number, in combination with any required security code, access code, or password that would permit access to any of the resident’s financial accounts.

History

[*Pub Acts 2018, No. 690*](#), effective January 20, 2021.

Michigan Compiled Laws Service
Copyright © 2020 Matthew Bender & Company, Inc.
a member of the LexisNexis Group. All rights reserved.

End of Document

MCLS § 500.563

This document is current through Public Act 1-192 from the 2020 Legislative Session

**Michigan Compiled Laws Service > Chapter 500 Insurance Code of 1956 (§§ 500.100 — 500.8302)
> Act 218 of 1956 (Chs. 1 — 83) > Chapter 5A Data Security [Effective January 20, 2021] (§§
500.550 — 500.565)**

§ 500.563. Confidential information. [Effective January 20, 2021]

Sec. 563.

(1) Any documents, materials, or other information in the control or possession of the department that is furnished by a licensee or an employee or agent of the licensee acting on behalf of the licensee under section 555(9), section 559(2)(b), (c), (d), (e), (h), (i), and (j), or that is obtained by the director in an investigation or examination by the director is confidential by law and privileged, is not subject to the freedom of information act, 1976 PA 442, [MCL 15.231](#) to [15.246](#), is not subject to subpoena, and is not subject to discovery or admissible in evidence in any private civil action. However, the director is authorized to use the documents, materials, or other information in the furtherance of any regulatory or legal action brought as a part of the director's duties. The director shall not otherwise make the documents, materials, or other information public.

(2) Neither the director nor any person that received documents, materials, or other information while acting under the authority of the director is permitted or required to testify in any private civil action concerning any confidential documents, materials, or information under subsection (1).

(3) To assist in the performance of the director's duties under this chapter, the director may do any of the following:

(a) Share documents, materials, or other information, including the confidential and privileged documents, materials, or information subject to subsection (1), with other state, federal, and international regulatory agencies, with the National Association of Insurance Commissioners, its affiliates, or its subsidiaries, and with state, federal, and international law enforcement authorities, if the recipient agrees in writing to maintain the confidentiality and privileged status of the document, material, or other information.

(b) Receive documents, materials, or information, including otherwise confidential and privileged documents, materials, or information, from the National Association of Insurance Commissioners, its affiliates, or its subsidiaries, and from regulatory and law enforcement officials of other foreign or domestic jurisdictions, and shall maintain as confidential or privileged any document, material, or information received with notice or the understanding that it is confidential or privileged under the laws of the jurisdiction that is the source of the document, material, or information.

(c) Share documents, materials, or other information subject to subsection (1) with a third-party consultant or vendor if the consultant agrees in writing to maintain the confidentiality and privileged status of the document, material, or other information.

(d) Enter into agreements governing sharing and use of information consistent with this subsection.

(4) A waiver of any applicable privilege or claim of confidentiality in the documents, materials, or information does not occur as a result of disclosure to the director under this section or as a result of sharing as authorized under subsection (3).

(5) This chapter does not prohibit the director from releasing final, adjudicated actions that are open to public inspection pursuant to the freedom of information act, 1976 PA 442, [MCL 15.231](#) to [15.246](#), to a database or

MCLS § 500.563

other clearinghouse service maintained by the National Association of Insurance Commissioners, its affiliates, or its subsidiaries.

(6) Any documents, materials, or other information in the possession or control of the National Association of Insurance Commissioners or a third-party consultant or vendor under this chapter is confidential by law and privileged, is not subject to the freedom of information act, 1976 PA 442, [MCL 15.231](#) to [15.246](#), is not subject to subpoena, and is not subject to discovery or admissible in evidence in any private civil action.

History

[Pub Acts 2018, No. 690](#), effective January 20, 2021.

Michigan Compiled Laws Service
Copyright © 2020 Matthew Bender & Company, Inc.
a member of the LexisNexis Group. All rights reserved.

End of Document

MCLS § 500.565

This document is current through Public Act 1-192 from the 2020 Legislative Session

**Michigan Compiled Laws Service > Chapter 500 Insurance Code of 1956 (§§ 500.100 — 500.8302)
> Act 218 of 1956 (Chs. 1 — 83) > Chapter 5A Data Security [Effective January 20, 2021] (§§
500.550 — 500.565)**

§ 500.565. Exemptions. [Effective January 20, 2021]

Sec. 565.

(1) A licensee that has fewer than 25 employees, including any independent contractors, is exempt from section 555.

(2) A licensee subject to and in compliance with the health insurance portability and accountability act of 1996, *Public Law 104-191*, and with regulations promulgated under that act, is not required to comply with this chapter except for the requirements under sections 559 and 561.

(3) An employee, agent, representative, or designee of a licensee, who is also a licensee, is exempt from section 555 and does not need to develop its own information security program to the extent that the employee, agent, representative, or designee is covered by the information security program of the other licensee.

(4) If a licensee ceases to qualify for the exception under subsection (1), the licensee has 180 days to comply with this chapter.

(5) This chapter takes effect on January 20, 2021. A licensee shall implement section 555 by January 20, 2022. However, a licensee has until January 20, 2023 to implement section 555(6).

History

[Pub Acts 2018, No. 690](#), effective January 20, 2021.

Michigan Compiled Laws Service
Copyright © 2020 Matthew Bender & Company, Inc.
a member of the LexisNexis Group. All rights reserved.

End of Document

Stop Hacks and Improve Electronic Data Security Act (SHIELD Act), 2019 **N.Y. SB 5575**

Chaptered, July 25, 2019

Reporter

2019 N.Y. ALS 117; 2019 N.Y. Laws 117; 2019 N.Y. Ch. 117; 2019 N.Y. SB 5575

**NEW YORK ADVANCE LEGISLATIVE SERVICE > NEW YORK 242ND ANNUAL LEGISLATIVE SESSION >
CHAPTER 117 > SENATE BILL 5575**

Notice

Added: Text highlighted in green

Deleted: Red text with a strikethrough

Synopsis

AN ACT to amend the general business law and the state technology law, in relation to notification of a security breach

Became a law July 25, 2019, with the approval of the Governor.

Passed by a majority vote, three-fifths being present.

Text

The People of the State of New York, represented in Senate and Assembly, do enact as follows:

Section 1.

This act shall be known and may be cited as the “Stop Hacks and Improve Electronic Data Security Act (**SHIELD Act**)”.

Section 2. The article heading of article 39-F of the general business law, as added by chapter 442 of the laws of 2005, is amended to read as follows:

NOTIFICATION OF UNAUTHORIZED ACQUISITION OF PRIVATE
INFORMATION; DATA SECURITY PROTECTIONS

Section 3. Subdivisions 1, 2, 3, 5, 6, 7 and 8 of section NY CLS [Gen Bus § 899-aa](#) of the general business law, subdivisions 1, 2, 3, 5, 6 and 7 as added by chapter 442 of the laws of 2005, paragraph (c) of subdivision 1,

Stop Hacks and Improve Electronic Data Security Act (SHIELD Act), 2019 N.Y. SB 5575

paragraph (a) of subdivision 6 and subdivision 8 as amended by chapter 491 of the laws of 2005 and paragraph (a) of subdivision 8 as amended by section 6 of part N of chapter 55 of the laws of 2013, are amended, subdivision 9 is renumbered subdivision 10 and a new subdivision 9 is added to read as follows:

1. As used in this section, the following terms shall have the following meanings:

- (a) "Personal information" shall mean any information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify such natural person;
- (b) "Private information" shall mean either: (i) personal information consisting of any information in combination with any one or more of the following data elements, when either the data element or the combination of personal information ~~or~~ plus the data element is not encrypted, or is encrypted with an encryption key that has also been accessed or acquired:
 - (1) social security number;
 - (2) driver's license number or non-driver identification card number; ~~or~~
 - (3) account number, credit or debit card number, in combination with any required security code, access code, ~~or~~ password or other information that would permit access to an individual's financial account;
 - (4) account number, credit or debit card number, if circumstances exist wherein such number could be used to access an individual's financial account without additional identifying information, security code, access code, or password; or
 - (5) biometric information, meaning data generated by electronic measurements of an individual's unique physical characteristics, such as a fingerprint, voice print, retina or iris image, or other unique physical representation or digital representation of biometric data which are used to authenticate or ascertain the individual's identity; or
- (ii) a user name or e-mail address in combination with a password or security question and answer that would permit access to an online account.

"Private information" does not include publicly available information which is lawfully made available to the general public from federal, state, or local government records.

- (c) "Breach of the security of the system" shall mean unauthorized access to or acquisition of, or access to or acquisition without valid authorization, of computerized data that compromises the security, confidentiality, or integrity of ~~personal~~ private information maintained by a business. Good faith access to, or acquisition of ~~personal~~, private information by an employee or agent of the business for the purposes of the business is not a breach of the security of the system, provided that the private information is not used or subject to unauthorized disclosure.

In determining whether information has been accessed, or is reasonably believed to have been accessed, by an unauthorized person or a person without valid authorization, such business may consider, among other factors, indications that the information was viewed, communicated with, used, or altered by a person without valid authorization or by an unauthorized person.

In determining whether information has been acquired, or is reasonably believed to have been acquired, by an unauthorized person or a person without valid authorization, such business may consider the following factors, among others:

- (1) indications that the information is in the physical possession and control of an unauthorized person, such as a lost or stolen computer or other device containing information; or
- (2) indications that the information has been downloaded or copied; or
- (3) indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported.

Stop Hacks and Improve Electronic Data Security Act (SHIELD Act), 2019 N.Y. SB 5575

- (d) "Consumer reporting agency" shall mean any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports. A list of consumer reporting agencies shall be compiled by the state attorney general and furnished upon request to any person or business required to make a notification under subdivision two of this section.
2. Any person or business which ~~conducts business in New York state, and which~~ owns or licenses computerized data which includes private information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the system to any resident of New York state whose private information was, or is reasonably believed to have been, **accessed or** acquired by a person without valid authorization. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision four of this section, or any measures necessary to determine the scope of the breach and restore the ~~reasonable~~ integrity of the system.
- (a) Notice to affected persons under this section is not required if the exposure of private information was an inadvertent disclosure by persons authorized to access private information, and the person or business reasonably determines such exposure will not likely result in misuse of such information, or financial harm to the affected persons or emotional harm in the case of unknown disclosure of online credentials as found in subparagraph (ii) of paragraph (b) of subdivision one of this section. Such a determination must be documented in writing and maintained for at least five years. If the incident affects over five hundred residents of New York, the person or business shall provide the written determination to the state attorney general within ten days after the determination.
- (b) If notice of the breach of the security of the system is made to affected persons pursuant to the breach notification requirements under any of the following laws, nothing in this section shall require any additional notice to those affected persons, but notice still shall be provided to the state attorney general, the department of state and the division of state police pursuant to paragraph (a) of subdivision eight of this section and to consumer reporting agencies pursuant to paragraph (b) of subdivision eight of this section:
- (i) regulations promulgated pursuant to Title V of the federal GrammLeach-Bliley Act (15 U.S.C. 6801 to 6809), as amended from time to time;
 - (ii) regulations implementing the Health Insurance Portability and Accountability Act of 1996 (45 C.F.R. parts 160 and 164), as amended from time to time, and the Health Information Technology for Economic and Clinical Health Act, as amended from time to time;
 - (iii) part five hundred of title twenty-three of the official compilation of codes, rules and regulations of the state of New York, as amended from time to time; or
 - (iv) any other data security rules and regulations of, and the statutes administered by, any official department, division, commission or agency of the federal or New York state government as such rules, regulations or statutes are interpreted by such department, division, commission or agency or by the federal or New York state courts.
3. Any person or business which maintains computerized data which includes private information which such person or business does not own shall notify the owner or licensee of the information of any breach of the security of the system immediately following discovery, if the private information was, or is reasonably believed to have been, **accessed or** acquired by a person without valid authorization.
5. The notice required by this section shall be directly provided to the affected persons by one of the following methods:
- (a) written notice;

Stop Hacks and Improve Electronic Data Security Act (SHIELD Act), 2019 N.Y. SB 5575

- (b) electronic notice, provided that the person to whom notice is required has expressly consented to receiving said notice in electronic form and a log of each such notification is kept by the person or business who notifies affected persons in such form; provided further, however, that in no case shall any person or business require a person to consent to accepting said notice in said form as a condition of establishing any business relationship or engaging in any transaction.
- (c) telephone notification provided that a log of each such notification is kept by the person or business who notifies affected persons; or
- (d) substitute notice, if a business demonstrates to the state attorney general that the cost of providing notice would exceed two hundred fifty thousand dollars, or that the affected class of subject persons to be notified exceeds five hundred thousand, or such business does not have sufficient contact information. Substitute notice shall consist of all of the following:
 - (1) e-mail notice when such business has an e-mail address for the subject persons, except if the breached information includes an e-mail address in combination with a password or security question and answer that would permit access to the online account, in which case the person or business shall instead provide clear and conspicuous notice delivered to the consumer online when the consumer is connected to the online account from an internet protocol address or from an online location which the person or business knows the consumer customarily uses to access the online account;
 - (2) conspicuous posting of the notice on such business's web site page, if such business maintains one; and
 - (3) notification to major statewide media.

6.

- (a) whenever the attorney general shall believe from evidence satisfactory to him or her that there is a violation of this article he or she may bring an action in the name and on behalf of the people of the state of New York, in a court of justice having jurisdiction to issue an injunction, to enjoin and restrain the continuation of such violation. In such action, preliminary relief may be granted under article sixty-three of the civil practice law and rules. In such action the court may award damages for actual costs or losses incurred by a person entitled to notice pursuant to this article, if notification was not provided to such person pursuant to this article, including consequential financial losses. Whenever the court shall determine in such action that a person or business violated this article knowingly or recklessly, the court may impose a civil penalty of the greater of five thousand dollars or up to ~~ten~~twenty dollars per instance of failed notification, provided that the latter amount shall not exceed ~~one~~two hundred fifty thousand dollars.
- (b) the remedies provided by this section shall be in addition to any other lawful remedy available.
- (c) no action may be brought under the provisions of this section unless such action is commenced within ~~two~~three years immediately after either the date ~~of the act complained of or the date of discovery of such act~~ on which the attorney general became aware of the violation, or the date of notice sent pursuant to paragraph (a) of subdivision eight of this section, whichever occurs first. In no event shall an action be brought after six years from the date of discovery of the breach of private information by the company unless the company took steps to hide the breach.

- 7. Regardless of the method by which notice is provided, such notice shall include contact information for the person or business making the notification, the telephone numbers and websites of the relevant state and federal agencies that provide information regarding security breach response and identity theft prevention and protection information, and a description of the categories of information that were, or are reasonably believed to have been, accessed or acquired by a person without valid authorization, including specification of which of the elements of personal information and private information were, or are reasonably believed to have been, so accessed or acquired.

8.

Stop Hacks and Improve Electronic Data Security Act (SHIELD Act), 2019 N.Y. SB 5575

- (a) In the event that any New York residents are to be notified, the person or business shall notify the state attorney general, the department of state and the division of state police as to the timing, content and distribution of the notices and approximate number of affected persons and shall provide a copy of the template of the notice sent to affected persons. Such notice shall be made without delaying notice to affected New York residents.
 - (b) In the event that more than five thousand New York residents are to be notified at one time, the person or business shall also notify consumer reporting agencies as to the timing, content and distribution of the notices and approximate number of affected persons. Such notice shall be made without delaying notice to affected New York residents.
9. Any covered entity required to provide notification of a breach, including breach of information that is not "private information" as defined in paragraph (b) of subdivision one of this section, to the secretary of health and human services pursuant to the Health Insurance Portability and Accountability Act of 1996 or the Health Information Technology for Economic and Clinical Health Act, as amended from time to time, shall provide such notification to the state attorney general within five business days of notifying the secretary.

Section 4. The general business law is amended by adding a new section 899–bb to read as follows:

§ 899-bb. Data security protections.

1. Definitions.

- (a) "Compliant regulated entity" shall mean any person or business that is subject to, and in compliance with, any of the following data security requirements:
 - (i) regulations promulgated pursuant to Title V of the federal GrammLeach-Bliley Act (15 U.S.C. 6801 to 6809), as amended from time to time;
 - (ii) regulations implementing the Health Insurance Portability and Accountability Act of 1996 (45 C.F.R. parts 160 and 164), as amended from time to time, and the Health Information Technology for Economic and Clinical Health Act, as amended from time to time;
 - (iii) part five hundred of title twenty-three of the official compilation of codes, rules and regulations of the state of New York, as amended from time to time; or
 - (iv) any other data security rules and regulations of, and the statutes administered by, any official department, division, commission or agency of the federal or New York state government as such rules, regulations or statutes are interpreted by such department, division, commission or agency or by the federal or New York state courts.
 - (b) "Private information" shall have the same meaning as defined in section eight hundred ninety-nine-aa of this article.
 - (c) "Small business" shall mean any person or business with (i) fewer than fifty employees; (ii) less than three million dollars in gross annual revenue in each of the last three fiscal years; or (iii) less than five million dollars in year-end total assets, calculated in accordance with generally accepted accounting principles.
2. Reasonable security requirement. (a) Any person or business that owns or licenses computerized data which includes private information of a resident of New York shall develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of the private information including, but not limited to, disposal of data.
- (b) A person or business shall be deemed to be in compliance with paragraph (a) of this subdivision if it either:
 - (i) is a compliant regulated entity as defined in subdivision one of this section; or
 - (ii) implements a data security program that includes the following:

Stop Hacks and Improve Electronic Data Security Act (SHIELD Act), 2019 N.Y. SB 5575

- (A) reasonable administrative safeguards such as the following, in which the person or business:
 - (1) designates one or more employees to coordinate the security program;
 - (2) identifies reasonably foreseeable internal and external risks;
 - (3) assesses the sufficiency of safeguards in place to control the identified risks;
 - (4) trains and manages employees in the security program practices and procedures;
 - (5) selects service providers capable of maintaining appropriate safeguards, and requires those safeguards by contract; and
 - (6) adjusts the security program in light of business changes or new circumstances; and
- (B) reasonable technical safeguards such as the following, in which the person or business:
 - (1) assesses risks in network and software design;
 - (2) assesses risks in information processing, transmission and storage;
 - (3) detects, prevents and responds to attacks or system failures; and
 - (4) regularly tests and monitors the effectiveness of key controls, systems and procedures; and
- (C) reasonable physical safeguards such as the following, in which the person or business:
 - (1) assesses risks of information storage and disposal;
 - (2) detects, prevents and responds to intrusions;
 - (3) protects against unauthorized access to or use of private information during or after the collection, transportation and destruction or disposal of the information; and
 - (4) disposes of private information within a reasonable amount of time after it is no longer needed for business purposes by erasing electronic media so that the information cannot be read or reconstructed.
- (c) A small business as defined in paragraph (c) of subdivision one of this section complies with subparagraph (ii) of paragraph (b) of subdivision two of this section if the small business's security program contains reasonable administrative, technical and physical safeguards that are appropriate for the size and complexity of the small business, the nature and scope of the small business's activities, and the sensitivity of the personal information the small business collects from or about consumers.
- (d) Any person or business that fails to comply with this subdivision shall be deemed to have violated section three hundred forty-nine of this chapter, and the attorney general may bring an action in the name and on behalf of the people of the state of New York to enjoin such violations and to obtain civil penalties under section three hundred fifty-d of this chapter.
- (e) Nothing in this section shall create a private right of action.

Section 5. Paragraph (a) of subdivision 1 and subdivisions 2, 3, 6, 7 and 8 of section NY CLS [STATE TECHNOLOGY LAW § 208](#) of the state technology law, paragraph (a) of subdivision 1 and subdivisions 3 and 8 as added by chapter 442 of the laws of 2005, subdivision 2 and paragraph (a) of subdivision 7 as amended by section 5 of part N of chapter 55 of the laws of 2013 and subdivisions 6 and 7 as amended by chapter 491 of the laws of 2005, are amended and a new subdivision 9 is added to read as follows:

- (a) "Private information" shall mean either:

Stop Hacks and Improve Electronic Data Security Act (SHIELD Act), 2019 N.Y. SB 5575

(i) personal information consisting of any information in combination with any one or more of the following data elements, when either the data element or the combination of personal information ~~or~~plus the data element is not encrypted or encrypted with an encryption key that has also been accessed or acquired:

(1) social security number;

(2) driver's license number or non-driver identification card number;~~or~~

(3) account number, credit or debit card number, in combination with any required security code, access code, ~~or~~password or other information which would permit access to an individual's financial account;

(4) account number, or credit or debit card number, if circumstances exist wherein such number could be used to access to an individual's financial account without additional identifying information, security code, access code, or password; or

(5) biometric information, meaning data generated by electronic measurements of an individual's unique physical characteristics, such as fingerprint, voice print, or retina or iris image, or other unique physical representation or digital representation which are used to authenticate or ascertain the individual's identity; or

(ii) a user name or e-mail address in combination with a password or security question and answer that would permit access to an online account.

"Private information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

2. Any state entity that owns or licenses computerized data that includes private information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the system to any resident of New York state whose private information was, or is reasonably believed to have been, accessed or acquired by a person without valid authorization. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision four of this section, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system. The state entity shall consult with the state office of information technology services to determine the scope of the breach and restoration measures. Within ninety days of the notice of the breach, the office of information technology services shall deliver a report on the scope of the breach and recommendations to restore and improve the security of the system to the state entity.

(a) Notice to affected persons under this section is not required if the exposure of private information was an inadvertent disclosure by persons authorized to access private information, and the state entity reasonably determines such exposure will not likely result in misuse of such information, or financial or emotional harm to the affected persons. Such a determination must be documented in writing and maintained for at least five years. If the incident affected over five hundred residents of New York, the state entity shall provide the written determination to the state attorney general within ten days after the determination.

(b) If notice of the breach of the security of the system is made to affected persons pursuant to the breach notification requirements under any of the following laws, nothing in this section shall require any additional notice to those affected persons, but notice still shall be provided to the state attorney general, the department of state and the office of information technology services pursuant to paragraph (a) of subdivision seven of this section and to consumer reporting agencies pursuant to paragraph (b) of subdivision seven of this section:

(i) regulations promulgated pursuant to Title V of the federal GrammLeach-Bliley Act (15 U.S.C. 6801 to 6809), as amended from time to time;

Stop Hacks and Improve Electronic Data Security Act (SHIELD Act), 2019 N.Y. SB 5575

- (ii) regulations implementing the Health Insurance Portability and Accountability Act of 1996 (45 C.F.R. parts 160 and 164), as amended from time to time, and the Health Information Technology for Economic and Clinical Health Act, as amended from time to time;
 - (iii) part five hundred of title twenty-three of the official compilation of codes, rules and regulations of the state of New York, as amended from time to time; or
 - (iv) any other data security rules and regulations of, and the statutes administered by, any official department, division, commission or agency of the federal or New York state government as such rules, regulations or statutes are interpreted by such department, division, commission or agency or by the federal or New York state courts.
3. Any state entity that maintains computerized data that includes private information which such agency does not own shall notify the owner or licensee of the information of any breach of the security of the system immediately following discovery, if the private information was, or is reasonably believed to have been, accessed or acquired by a person without valid authorization.
6. Regardless of the method by which notice is provided, such notice shall include contact information for the state entity making the notification, the telephone numbers and websites of the relevant state and federal agencies that provide information regarding security breach response and identity theft prevention and protection information and a description of the categories of information that were, or are reasonably believed to have been, accessed or acquired by a person without valid authorization, including specification of which of the elements of personal information and private information were, or are reasonably believed to have been, so accessed or acquired.
- 7.
- (a) In the event that any New York residents are to be notified, the state entity shall notify the state attorney general, the department of state and the state office of information technology services as to the timing, content and distribution of the notices and approximate number of affected persons and provide a copy of the template of the notice sent to affected persons. Such notice shall be made without delaying notice to affected New York residents.
 - (b) In the event that more than five thousand New York residents are to be notified at one time, the state entity shall also notify consumer reporting agencies as to the timing, content and distribution of the notices and approximate number of affected persons. Such notice shall be made without delaying notice to affected New York residents.
8. The state office of information technology services shall develop, update and provide regular training to all state entities relating to best practices for the prevention of a breach of the security of the system.
9. Any covered entity required to provide notification of a breach, including breach of information that is not "private information" as defined in paragraph (a) of subdivision one of this section, to the secretary of health and human services pursuant to the Health Insurance Portability and Accountability Act of 1996 or the Health Information Technology for Economic and Clinical Health Act, as amended from time to time, shall provide such notification to the state attorney general within five business days of notifying the secretary.
10. Any entity listed in subparagraph two of paragraph (c) of subdivision one of this section shall adopt a notification policy no more than one hundred twenty days after the effective date of this section. Such entity may develop a notification policy which is consistent with this section or alternatively shall adopt a local law which is consistent with this section.

Section 6.

This act shall take effect on the ninetieth day after it shall have become a law; provided, however, that section four of this act shall take effect on the two hundred fortieth day after it shall have become a law.

History

Approved by the Governor July 25, 2019

Effective date: October 23, 2019

Sponsor

Thomas

NEW YORK ADVANCE LEGISLATIVE SERVICE
Copyright © 2020 LexisNexis. All rights reserved.

End of Document

ORS § 646A.604

The Oregon Annotated Statutes is current through the 2020 Second Special Session. Some sections may have multiple variants due to amendments by multiple acts. Revision and codification by the Legislative Counsel are updated as available, see ORS 173.111 et seq. For sections pending codification by the Legislative Counsel, see Newly Added Sections in the Table of Contents.

LexisNexis® Oregon Annotated Statutes > Title 50 Trade Regulations and Practices (Chs. 645 — 650) > Chapter 646A- Trade Regulation (§§ 646A.010 — 646A.813) > Identity Theft Prevention (§§ 646A.600 — 646A.628)

646A.604 Notice of breach of security; delay; methods of notification; contents of notice; application of notice requirement.

(1) If a covered entity is subject to a breach of security or receives notice of a breach of security from a vendor, the covered entity shall give notice of the breach of security to:

(a) The consumer to whom the personal information pertains.

(b) The Attorney General, either in writing or electronically, if the number of consumers to whom the covered entity must send the notice described in paragraph (a) of this subsection exceeds 250.

(2)

(a) A vendor that discovers a breach of security or has reason to believe that a breach of security has occurred shall notify a covered entity with which the vendor has a contract as soon as is practicable but not later than 10 days after discovering the breach of security or having a reason to believe that the breach of security occurred.

(b) If a vendor has a contract with another vendor that, in turn, has a contract with a covered entity, the vendor shall notify the other vendor of a breach of security as provided in paragraph (a) of this subsection.

(c) A vendor shall notify the Attorney General in writing or electronically if the vendor was subject to a breach of security that involved the personal information of more than 250 consumers or a number of consumers that the vendor could not determine. This paragraph does not apply to the vendor if the covered entity described in paragraph (a) or (b) of this subsection has notified the Attorney General in accordance with the requirements of this section.

(3)

(a) A covered entity shall give notice of a breach of security in the most expeditious manner possible, without unreasonable delay, but not later than 45 days after discovering or receiving notification of the breach of security.

(b) Before providing the notice described in paragraph (a) of this subsection, a covered entity shall undertake reasonable measures that are necessary to:

(A) Determine sufficient contact information for the intended recipient of the notice;

(B) Determine the scope of the breach of security; and

(C) Restore the reasonable integrity, security and confidentiality of the personal information.

ORS § 646A.604

(c) A covered entity may delay giving the notice described in paragraph (a) of this subsection only if a law enforcement agency determines that a **notification** will impede a criminal investigation and if the law enforcement agency requests in writing that the covered entity delay the **notification**.

(4) A covered entity may notify a consumer of a **breach** of security:

(a) In writing;

(b) Electronically, if the covered entity customarily communicates with the consumer electronically or if the notice is consistent with the provisions regarding electronic records and signatures set forth in the Electronic Signatures in Global and National Commerce Act (15 U.S.C. 7001) as that Act existed on the effective date of this 2019 Act;

(c) By telephone, if the covered entity contacts the affected consumer directly; or

(d) With substitute notice, if the covered entity demonstrates that the cost of **notification** otherwise would exceed \$250,000 or that the affected class of consumers exceeds 350,000, or if the covered entity does not have sufficient contact information to notify affected consumers. For the purposes of this paragraph, "substitute notice" means:

(A) Posting the notice or a link to the notice conspicuously on the covered entity's website if the covered entity maintains a website; and

(B) Notifying major statewide television and newspaper media.

(5) Notice under this section must include, at a minimum:

(a) A description of the **breach** of security in general terms;

(b) The approximate date of the **breach** of security;

(c) The type of personal information that was subject to the **breach** of security;

(d) Contact information for the covered entity;

(e) Contact information for national consumer reporting agencies; and

(f) Advice to the consumer to report suspected identity theft to law enforcement, including the Attorney General and the Federal Trade Commission.

(6) If a covered entity discovers or receives notice of a **breach** of security that affects more than 1,000 consumers, the covered entity shall notify, without unreasonable delay, all consumer reporting agencies that compile and maintain reports on consumers on a nationwide basis of the timing, distribution and content of the notice the covered entity gave to affected consumers and shall include in the notice any police report number assigned to the **breach** of security. A covered entity may not delay notifying affected consumers of a **breach** of security in order to notify consumer reporting agencies.

(7)

(a) If a covered entity must notify a consumer of a **breach** of security under this section, and in connection with the **notification** the covered entity or an agent or affiliate of the covered entity offers to provide credit monitoring services or identity theft prevention and mitigation services without charge to the consumer, the covered entity, the agent or the affiliate may not condition the provision of the services on the consumer's providing the covered entity, the agent or the affiliate with a credit or debit card number or on the consumer's acceptance of any other service the covered entity offers to provide for a fee.

(b) If a covered entity or an agent or affiliate of the covered entity offers additional credit monitoring services or identity theft prevention and mitigation services for a fee to a consumer under the circumstances described in paragraph (a) of this subsection, the covered entity, the agent or the affiliate must separately, distinctly, clearly and conspicuously disclose in the offer for the additional

ORS § 646A.604

credit monitoring services or identity theft prevention and mitigation services that the covered entity, the agent or the affiliate will charge the consumer a fee.

(c) The terms and conditions of any contract under which one person offers or provides credit monitoring services or identity theft prevention and mitigation services on behalf of another person under the circumstances described in paragraph (a) of this subsection must require compliance with the requirements of paragraphs (a) and (b) of this subsection.

(8) Notwithstanding subsection (1) of this section, a covered entity does not need to notify consumers of a **breach** of security if, after an appropriate investigation or after consultation with relevant federal, state or local law enforcement agencies, the covered entity reasonably determines that the consumers whose personal information was subject to the **breach** of security are unlikely to suffer harm. The covered entity must document the determination in writing and maintain the documentation for at least five years.

(9) This section does not apply to:

(a) Personal information that is subject to, and a person that complies with, **notification** requirements or procedures for a **breach** of security that the person's primary or functional federal regulator adopts, promulgates or issues in rules, regulations, procedures, guidelines or guidance, if the personal information and the person would otherwise be subject to [ORS 646A.600](#) to [646A.628](#).

(b) Personal information that is subject to, and a person that complies with, a state or federal law that provides greater protection to personal information and disclosure requirements at least as thorough as the protections and disclosure requirements provided under this section.

(c) A covered entity or vendor that complies with regulations promulgated under Title V of the Gramm-Leach-Bliley Act of 1999 (15 U.S.C. 6801 to 6809) as that Act existed on the effective date of this 2019 Act, if personal information that is subject to [ORS 646A.600](#) to [646A.628](#) is also subject to that Act.

(d) A covered entity or vendor that complies with regulations promulgated under the Health Insurance Portability and Accountability Act of 1996 (*P.L. 104-191, 110 Stat. 1936*) and the Health Information Technology for Economic and Clinical Health Act of 2009 (*P.L. 111-5, Title XIII, 123 Stat. 226*), as those Acts existed on the effective date of this 2019 Act, if personal information that is subject to [ORS 646A.600](#) to [646A.628](#) is also subject to those Acts.

(10) Notwithstanding the exemptions set forth in subsection (9) of this section, a person, a covered entity or a vendor shall provide to the Attorney General within a reasonable time at least one copy of any notice the person, the covered entity or the vendor sends to consumers or to the person's, the covered entity's or the vendor's primary or functional regulator in compliance with this section or with other state or federal laws or regulations that apply to the person, the covered entity or the vendor as a consequence of a **breach** of security, if the **breach** of security affects more than 250 consumers.

(11)

(a) A person's violation of a provision of [ORS 646A.600](#) to [646A.628](#) is an unlawful practice under [ORS 646.607](#).

(b) A covered entity or vendor in an action or proceeding may affirmatively defend against an allegation that the covered entity or vendor has not developed, implemented and maintained reasonable safeguards to protect the security, confidentiality and integrity of personal information that is subject to [ORS 646A.600](#) to [646A.628](#) but is not subject to an Act described in subsection (9)(c) or (d) of this section by showing that, with respect to the personal information that is subject to [ORS 646A.600](#) to [646A.628](#), the covered entity or vendor developed, implemented and maintained reasonable security measures that would be required for personal information subject to the applicable Act.

(c) The rights and remedies available under this section are cumulative and are in addition to any other rights or remedies that are available under law.

History

[2007 c.759 § 3](#); [2015 c.357 § 2](#), effective January 1, 2016; [2018 c.10 § 2](#), effective June 2, 2018; [2019 c.180 § 3](#), effective January 1, 2020.

Annotations

Notes

Amendment Notes

The 2018 amendment by c. 10, § 2 (S.B. 1551), effective June 2, 2018, rewrote the section.

The 2019 amendment by c. 180 § 3 (SB 684), effective January 1, 2020, rewrote the section.

Applicability

Stats [2018 c.10 § 7](#) provides:

Sec. 7. The amendments to [ORS 646A.602](#), [646A.604](#), [646A.606](#), [646A.608](#), [646A.610](#) and [646A.622](#) by sections 1 to 6 of this 2018 Act apply to contracts into which a person enters with another person on or after the effective date of this 2018 Act.

LexisNexis® Oregon Annotated Statutes
Copyright © 2020 All rights reserved.

End of Document

Tex. Bus. & Com. Code § 521.053

This document is current through the most recent legislation which is the 2019 Regular Session, 86th Legislature, and the 2019 election results.

Texas Statutes & Codes Annotated by LexisNexis® > Business and Commerce Code > Title 11 Personal Identity Information (Subts. A — B) > Subtitle B Identity Theft (Chs. 521 — 523) > Chapter 521 Unauthorized Use of Identifying Information (Subchs. A — D) > Subchapter B Identity Theft (§§ 521.051 — 521.100)

Sec. 521.053. Notification Required Following Breach of Security of Computerized Data.

(a)In this section, “breach of system security” means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive personal information maintained by a person, including data that is encrypted if the person accessing the data has the key required to decrypt the data. Good faith acquisition of sensitive personal information by an employee or agent of the person for the purposes of the person is not a breach of system security unless the person uses or discloses the sensitive personal information in an unauthorized manner.

(b)A person who conducts business in this state and owns or licenses computerized data that includes sensitive personal information shall disclose any breach of system security, after discovering or receiving notification of the breach, to any individual whose sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made without unreasonable delay and in each case not later than the 60th day after the date on which the person determines that the breach occurred, except as provided by Subsection (d) or as necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(b-1)If the individual whose sensitive personal information was or is reasonably believed to have been acquired by an unauthorized person is a resident of a state that requires a person described by Subsection (b) to provide notice of a breach of system security, the notice of the breach of system security required under Subsection (b) may be provided under that state’s law or under Subsection (b).

(c)Any person who maintains computerized data that includes sensitive personal information not owned by the person shall notify the owner or license holder of the information of any breach of system security immediately after discovering the breach, if the sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(d)A person may delay providing notice as required by Subsection (b) or (c) at the request of a law enforcement agency that determines that the notification will impede a criminal investigation. The notification shall be made as soon as the law enforcement agency determines that the notification will not compromise the investigation.

(e)A person may give notice as required by Subsection (b) or (c) by providing:

- (1)**written notice at the last known address of the individual;
- (2)**electronic notice, if the notice is provided in accordance with [15 U.S.C. Section 7001](#); or
- (3)**notice as provided by Subsection (f).

(f)If the person required to give notice under Subsection (b) or (c) demonstrates that the cost of providing notice would exceed \$250,000, the number of affected persons exceeds 500,000, or the person does not have sufficient contact information, the notice may be given by:

- (1) electronic mail, if the person has electronic mail addresses for the affected persons;
- (2) conspicuous posting of the notice on the person's website; or
- (3) notice published in or broadcast on major statewide media.

(g) Notwithstanding Subsection (e), a person who maintains the person's own notification procedures as part of an information security policy for the treatment of sensitive personal information that complies with the timing requirements for notice under this section complies with this section if the person notifies affected persons in accordance with that policy.

(h) If a person is required by this section to notify at one time more than 10,000 persons of a breach of system security, the person shall also notify each consumer reporting agency, as defined by [15 U.S.C. Section 1681a](#), that maintains files on consumers on a nationwide basis, of the timing, distribution, and content of the notices. The person shall provide the notice required by this subsection without unreasonable delay.

(i) A person who is required to disclose or provide notification of a breach of system security under this section shall notify the attorney general of that breach not later than the 60th day after the date on which the person determines that the breach occurred if the breach involves at least 250 residents of this state. The notification under this subsection must include:

- (1) a detailed description of the nature and circumstances of the breach or the use of sensitive personal information acquired as a result of the breach;
- (2) the number of residents of this state affected by the breach at the time of notification;
- (3) the measures taken by the person regarding the breach;
- (4) any measures the person intends to take regarding the breach after the notification under this subsection; and
- (5) information regarding whether law enforcement is engaged in investigating the breach.

History

Enacted by [Acts 2007, 80th Leg., ch. 885 \(H.B. 2278\), § 2.01](#), effective April 1, 2009; am. [Acts 2009, 81st Leg., ch. 419 \(H.B. 2004\), § 3](#), effective September 1, 2009; am. [Acts 2011, 82nd Leg., ch. 1126 \(H.B. 300\), § 14](#), effective September 1, 2012; am. Acts 2013, 83rd Leg., ch. 1368 (S.B. 1610), § 1, effective June 14, 2013; am. [Acts 2019, 86th Leg., ch. 1326 \(H.B. 4390\), § 1](#), effective January 1, 2020.

Annotations

LexisNexis® Notes

Notes

STATUTORY NOTES

Amendment Notes

2009 amendment, added "including data that is encrypted if the person accessing the data has the key required to decrypt the data" in the first sentence of (a).

2011 amendment, substituted “individual” for “resident of this state” in the first sentence of (b); and added (b-1).

2013 amendment, in (b-1), deleted “Notwithstanding Subsection (b), the requirements of Subsection (b) apply only” at the beginning, deleted “of this state or another state that does not require a person described by Subsection (b) to notify the individual of a breach of system security. If the individual is a resident” after “is a resident,” added “required under Subsection (b) may be,” and substituted “or under” for “satisfies the requirements of”; added “at the last known address of the individual” in (e)(1); and made a related change.

The 2019 amendment substituted “without unreasonable delay and in each case not later than the 60th day after the date on which the person determines that the breach occurred” for “as quickly as possible” in the second sentence of (b) and added (i).

Applicability

Acts 2009, 81st Leg., ch. 419 (**H.B. 2004**), § 7 provides: “The changes in law made by this Act apply only to a breach of system security that occurs on or after the effective date of this Act [September 1, 2009]. A breach of system security that occurs before the effective date of this Act is governed by the law in effect on the date the breach occurred, and the former law is continued in effect for that purpose.”

[*Acts 2011, 82nd Leg., ch. 1126 \(H.B. 300\), § 25*](#) provides: “The changes in law made by [Section 181.201, Health and Safety Code](#), as amended by this Act, [Section 521.053, Business & Commerce Code](#), as amended by this Act, and [Section 521.151\(a-1\), Business & Commerce Code](#), as added by this Act, apply only to conduct that occurs on or after the effective date of this Act [September 1, 2012]. Conduct that occurs before the effective date of this Act is governed by the law in effect at the time the conduct occurred, and the former law is continued in effect for that purpose.”

Case Notes

Banking Law: Consumer Protection: Fair Credit Reporting: Identity Theft

Person responsible for notice under the statute and rule is different, the contents and purpose of the notice under the statute and rule is different, the stage in the proceedings for giving notice under the statute and rule is different, and the appropriate person to bear the cost of notice under the statute and rule is different; the trial court erred in determining that an obligation to give statutory notice equated to an obligation to give notice under the rule. [*Bliss & Glennon Inc. v. Ashley*, 420 S.W.3d 379, 2014 Tex. App. LEXIS 112 \(Tex. App. Houston 1st Dist. Jan. 7, 2014, no pet.\)](#).

Company’s petition revealed no more than the desire to take a prudent approach to identifying data and protect and notify those impacted if necessary, and the company was not in position to know what materials, if any, were covered by the chapter, and thus the company did not judicially admit that it committed a data breach or that it was required to give a particular form of notice. [*Bliss & Glennon Inc. v. Ashley*, 420 S.W.3d 379, 2014 Tex. App. LEXIS 112 \(Tex. App. Houston 1st Dist. Jan. 7, 2014, no pet.\)](#).

End of Document

9 V.S.A. § 2430

Statutes current with Titles 1, 3A-9A, 10A-12, 14-15C, 16A-17, 19-22, and 24A-33 current with Legislation through Act 150 of the 2019 (Adj. Sess.) and Municipal Act M-11 of the 2019 (Adj. Sess.); Titles 2-3, 10, 13, 16, 18, and 23-24 current with Legislation through Act 130 of the 2019 (Adj. Sess.) and Municipal Act M-11 of the 2019 (Adj. Sess.)

VT - Vermont Statutes Annotated > TITLE NINE. COMMERCE AND TRADE > PART 3. SALES, ASSIGNMENTS, AND SECURED TRANSACTIONS > CHAPTER 62. PROTECTION OF PERSONAL INFORMATION > SUBCHAPTER 1. GENERAL PROVISIONS

§ 2430. Definitions

As used in this chapter:

(1)(A) "Brokered personal information" means one or more of the following computerized data elements about a consumer, if categorized or organized for dissemination to third parties:

(i)name;

(ii)address;

(iii)date of birth;

(iv)place of birth;

(v)mother's maiden name;

(vi)unique biometric data generated from measurements or technical analysis of human body characteristics used by the owner or licensee of the data to identify or authenticate the consumer, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data;

(vii)name or address of a member of the consumer's immediate family or household;

(viii)Social Security number or other government-issued identification number; or

(ix)other information that, alone or in combination with the other information sold or licensed, would allow a reasonable person to identify the consumer with reasonable certainty.

(B)"Brokered personal information" does not include publicly available information to the extent that it is related to a consumer's business or profession.

(2)"Business" means a commercial entity, including a sole proprietorship, partnership, corporation, association, limited liability company, or other group, however organized and whether or not organized to operate at a profit, including a financial institution organized, chartered, or holding a license or authorization certificate under the laws of this State, any other state, the United States, or any other country, or the parent, affiliate, or subsidiary of a financial institution, but does not include the State, a State agency, any political subdivision of the State, or a vendor acting solely on behalf of, and at the direction of, the State.

(3)"Consumer" means an individual residing in this State.

(4)(A) "Data broker" means a business, or unit or units of a business, separately or together, that knowingly collects and sells or licenses to third parties the brokered personal information of a consumer with whom the business does not have a direct relationship.

(B)Examples of a direct relationship with a business include if the consumer is a past or present:

9 V.S.A. § 2430

- (i) customer, client, subscriber, user, or registered user of the business's goods or services;
- (ii) employee, contractor, or agent of the business;
- (iii) investor in the business; or
- (iv) donor to the business.

(C) The following activities conducted by a business, and the collection and sale or licensing of brokered personal information incidental to conducting these activities, do not qualify the business as a data broker:

- (i) developing or maintaining third-party e-commerce or application platforms;
- (ii) providing 411 directory assistance or directory information services, including name, address, and telephone number, on behalf of or as a function of a telecommunications carrier;
- (iii) providing publicly available information related to a consumer's business or profession; or
- (iv) providing publicly available information via real-time or near-real-time alert services for health or safety purposes.

(D) The phrase "sells or licenses" does not include:

- (i) a one-time or occasional sale of assets of a business as part of a transfer of control of those assets that is not part of the ordinary conduct of the business; or
- (ii) a sale or license of data that is merely incidental to the business.

(5)(A) "Data broker security breach" means an unauthorized acquisition or a reasonable belief of an unauthorized acquisition of more than one element of brokered personal information maintained by a data broker when the brokered personal information is not encrypted, redacted, or protected by another method that renders the information unreadable or unusable by an unauthorized person.

(B) "Data broker security breach" does not include good faith but unauthorized acquisition of brokered personal information by an employee or agent of the data broker for a legitimate purpose of the data broker, provided that the brokered personal information is not used for a purpose unrelated to the data broker's business or subject to further unauthorized disclosure.

(C) In determining whether brokered personal information has been acquired or is reasonably believed to have been acquired by a person without valid authorization, a data broker may consider the following factors, among others:

- (i) indications that the brokered personal information is in the physical possession and control of a person without valid authorization, such as a lost or stolen computer or other device containing brokered personal information;
- (ii) indications that the brokered personal information has been downloaded or copied;
- (iii) indications that the brokered personal information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported; or
- (iv) that the brokered personal information has been made public.

(6) "Data collector" means a person who, for any purpose, whether by automated collection or otherwise, handles, collects, disseminates, or otherwise deals with personally identifiable information, and includes the State, State agencies, political subdivisions of the State, public and private universities, privately and publicly held corporations, limited liability companies, financial institutions, and retail operators.

(7) "Encryption" means use of an algorithmic process to transform data into a form in which the data is rendered unreadable or unusable without use of a confidential process or key.

9 V.S.A. § 2430

(8)"License" means a grant of access to, or distribution of, data by one person to another in exchange for consideration. A use of data for the sole benefit of the data provider, where the data provider maintains control over the use of the data, is not a license.

(9)"Login credentials" means a consumer's user name or e-mail address, in combination with a password or an answer to a security question, that together permit access to an online account.

(10)(A) "Personally identifiable information" means a consumer's first name or first initial and last name in combination with one or more of the following digital data elements, when the data elements are not encrypted, redacted, or protected by another method that renders them unreadable or unusable by unauthorized persons:

(i)a Social Security number;

(ii)a driver license or nondriver State identification card number, individual taxpayer identification number, passport number, military identification card number, or other identification number that originates from a government identification document that is commonly used to verify identity for a commercial transaction;

(iii)a financial account number or credit or debit card number, if the number could be used without additional identifying information, access codes, or passwords;

(iv)a password, personal identification number, or other access code for a financial account;

(v)unique biometric data generated from measurements or technical analysis of human body characteristics used by the owner or licensee of the data to identify or authenticate the consumer, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data;

(vi)genetic information; and

(vii)

(I)health records or records of a wellness program or similar program of health promotion or disease prevention;

(II)a health care professional's medical diagnosis or treatment of the consumer; or

(III)a health insurance policy number.

(B)"Personally identifiable information" does not mean publicly available information that is lawfully made available to the general public from federal, State, or local government records.

(11)"Record" means any material on which written, drawn, spoken, visual, or electromagnetic information is recorded or preserved, regardless of physical form or characteristics.

(12)"Redaction" means the rendering of data so that the data are unreadable or are truncated so that no more than the last four digits of the identification number are accessible as part of the data.

(13)(A) "Security breach" means unauthorized acquisition of electronic data, or a reasonable belief of an unauthorized acquisition of electronic data, that compromises the security, confidentiality, or integrity of a consumer's personally identifiable information or login credentials maintained by a data collector.

(B)"Security breach" does not include good faith but unauthorized acquisition of personally identifiable information or login credentials by an employee or agent of the data collector for a legitimate purpose of the data collector, provided that the personally identifiable information or login credentials are not used for a purpose unrelated to the data collector's business or subject to further unauthorized disclosure.

9 V.S.A. § 2430

(C)In determining whether personally identifiable information or login credentials have been acquired or is reasonably believed to have been acquired by a person without valid authorization, a data collector may consider the following factors, among others:

- (i)**indications that the information is in the physical possession and control of a person without valid authorization, such as a lost or stolen computer or other device containing information;
- (ii)**indications that the information has been downloaded or copied;
- (iii)**indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported; or
- (iv)**that the information has been made public.

History

Added [2005, No. 162](#) (Adj. Sess.), § 1, eff. Jan. 1, 2007; amended [2011, No. 109](#) (Adj. Sess.), § 4, eff. May 8, 2012; 2017, No. 171 (Adj. Sess.), § 2, eff. Jan. 1, 2019.; 2019, No. 89 (Adj. Sess.), § 2.

Annotations

Notes

HISTORY

REVISION NOTE.

--2013. In subdiv. (3), deleted ", but is not limited to" following "include" in accordance with [2013, No. 5](#), § 4.

AMENDMENTS--

2019 (ADJ. SESS.). Subdivision (9): Added.

Redesignated former subdiv. (9) through subdiv. (12) as subdiv. (10) through subdiv. (13).

Subdiv. (10)(A): Rewritten.

Inserted "or login credentials" following "identifiable information" in subdivs. (13)(A) and (13)(B); in subdiv. (13)(B), substituted "or login credentials are" for "is".

Subdiv. (13)(C): Substituted "or login credentials have" for "has" in the introductory language.

--2017 (ADJ. SESS.). Section amended generally.

--2011 (ADJ. SESS.). Subdiv. (5): Substituted "personally identifiable information" for "personal information" throughout.

Subdiv. (8)(A): Deleted "or access" following "acquisition"; substituted "electronic" for "computerized" preceding "data"; inserted "or a reasonable belief of an unauthorized acquisition of electronic data" following "data" and substituted "a consumer's personally identifiable" for "personal" preceding "information".

Subdiv. (8)(B): Substituted "personally identifiable" for "personal" preceding "information" in two places.

Subdiv. (8)(C): Added.

HISTORY

REVISION NOTE.

--2012. Substituted "commissioner of financial regulation" for "commissioner of banking, insurance, securities, and health care administration" and "department of financial regulation" for "department of banking, insurance, securities, and health care administration" throughout the title in accordance with [2011, No. 78](#) (Adj. Sess.), § 2.

Research References & Practice Aids

NOTES APPLICABLE TO ENTIRE TITLE

Copyright 2020 by LEGISLATIVE COUNCIL OF THE GENERAL ASSEMBLY FOR THE STATE OF VERMONT

End of Document

[Rev. Code Wash. \(ARCW\) § 19.255.010](#)

Statutes current with legislation from the 2020 Regular Session

Annotated Revised Code of Washington > Title 19 Business Regulations — Miscellaneous (Chs. 19.02 — Chapter 19.405) > Chapter 19.255 Personal Information — Notice of Security Breaches (§§ 19.255.005 — 19.255.040)

19.255.010. Personal information — Notice of security breaches.

(1) Any person or business that conducts business in this state and that owns or licenses data that includes personal information shall disclose any breach of the security of the system to any resident of this state whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person and the personal information was not secured. Notice is not required if the breach of the security of the system is not reasonably likely to subject consumers to a risk of harm. The breach of secured personal information must be disclosed if the information acquired and accessed is not secured during a security breach or if the confidential process, encryption key, or other means to decipher the secured information was acquired by an unauthorized person.

(2) Any person or business that maintains or possesses data that may include personal information that the person or business does not own or license shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(3) The notification required by this section may be delayed if the data owner or licensee contacts a law enforcement agency after discovery of a breach of the security of the system and a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.

(4) For purposes of this section and except under subsection (5) of this section and [RCW 19.255.030](#), notice may be provided by one of the following methods:

(a) Written notice;

(b) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in [15 U.S.C. Sec. 7001](#);

(c) Substitute notice, if the person or business demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars, or that the affected class of subject persons to be notified exceeds five hundred thousand, or the person or business does not have sufficient contact information. Substitute notice shall consist of all of the following:

(i) Email notice when the person or business has an email address for the subject persons;

(ii) Conspicuous posting of the notice on the web site page of the person or business, if the person or business maintains one; and

(iii) Notification to major statewide media; or

(d)

(i) If the breach of the security of the system involves personal information including a user name or password, notice may be provided electronically or by email. The notice must comply with subsections (6), (7), and (8) of this section and must inform the person whose personal information has been breached to promptly change his or her password and security question or answer, as

applicable, or to take other appropriate steps to protect the online account with the person or business and all other online accounts for which the person whose personal information has been **breached** uses the same user name or email address and password or security question or answer;

(ii) However, when the **breach** of the security of the system involves login credentials of an email account furnished by the person or business, the person or business may not provide the **notification** to that email address, but must provide notice using another method described in this subsection (4). The notice must comply with subsections (6), (7), and (8) of this section and must inform the person whose personal information has been **breached** to promptly change his or her password and security question or answer, as applicable, or to take other appropriate steps to protect the online account with the person or business and all other online accounts for which the person whose personal information has been **breached** uses the same user name or email address and password or security question or answer.

(5) A person or business that maintains its own **notification** procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this section is in compliance with the **notification** requirements of this section if the person or business notifies subject persons in accordance with its policies in the event of a **breach** of security of the system.

(6) Any person or business that is required to issue **notification** pursuant to this section shall meet all of the following requirements:

(a) The **notification** must be written in plain language; and

(b) The **notification** must include, at a minimum, the following information:

(i) The name and contact information of the reporting person or business subject to this section;

(ii) A list of the types of personal information that were or are reasonably believed to have been the subject of a **breach**;

(iii) A time frame of exposure, if known, including the date of the **breach** and the date of the discovery of the **breach**; and

(iv) The toll-free telephone numbers and addresses of the major credit reporting agencies if the **breach** exposed personal information.

(7) Any person or business that is required to issue a **notification** pursuant to this section to more than five hundred Washington residents as a result of a single **breach** shall notify the attorney general of the **breach** no more than thirty days after the **breach** was discovered.

(a) The notice to the attorney general shall include the following information:

(i) The number of Washington consumers affected by the **breach**, or an estimate if the exact number is not known;

(ii) A list of the types of personal information that were or are reasonably believed to have been the subject of a **breach**;

(iii) A time frame of exposure, if known, including the date of the **breach** and the date of the discovery of the **breach**;

(iv) A summary of steps taken to contain the **breach**; and

(v) A single sample copy of the security **breach notification**, excluding any personally identifiable information.

(b) The notice to the attorney general must be updated if any of the information identified in (a) of this subsection is unknown at the time notice is due.

(8)Notification to affected consumers under this section must be made in the most expedient time possible, without unreasonable delay, and no more than thirty calendar days after the **breach** was discovered, unless the delay is at the request of law enforcement as provided in subsection (3) of this section, or the delay is due to any measures necessary to determine the scope of the **breach** and restore the reasonable integrity of the data system.

History

[2019 c 241, § 2](#), effective March 1, 2020; [2015 c 64, § 2](#), effective July 24, 2015; 2005 c 368 § [2](#).

Annotations

Notes

Amendment Notes

2019 c 241 § 2, effective March 1, 2020, rewrote the section.

2015 c 64 § 2, effective July 24, 2015, rewrote the section.

Research References & Practice Aids

Hierarchy Notes:

[Rev. Code Wash. \(ARCW\) Title 19](#)

State Notes

Notes

Effective date — [2019 c 241](#):

“This act takes effect March 1, 2020.” [[2019 c 241 § 8](#).]

Effective date — [2019 c 241](#):

“This act takes effect March 1, 2020.” [[2019 c 241 § 8](#).]

Intent — [2015 c 64](#):

“The legislature recognizes that data **breaches** of personal information can compromise financial security and be costly to consumers. The legislature intends to strengthen the data **breach notification** requirements to better safeguard personal information, prevent identity theft, and ensure that the attorney general receives **notification** when **breaches** occur so that appropriate action may be taken to protect consumers. The legislature also intends to provide consumers whose personal information has been jeopardized due to a data **breach** with the information needed to secure financial accounts and make the necessary reports in a timely manner to minimize harm from identity theft.” [[2015 c 64 § 1](#).]

Research References & Practice Aids

Cross references.

Similar provision: [RCW 42.56.590](#).

Annotated Revised Code of Washington
Copyright © 2020 Matthew Bender & Company, Inc.,
a member of the LexisNexis Group. All rights reserved.

End of Document