Suggested Amendments to the

Alaska Consumer Data Privacy Act (Senate Bill 116/House Bill 159) ("ACPA")

Submitted by

Chris Koa, JD, MPA, CIPP/US, Europe & Canada
DataEsque Law Group PLLC
(chris@dataesquelaw.com)

for Lynden Incorporated

April ~~1~~20, 2021 3 pm DRAFT

SENATE BILL NO. 116

IN THE LEGISLATURE OF THE STATE OF ALASKA

THIRTY-SECOND LEGISLATURE - FIRST SESSION

BY THE SENATE RULES COMMITTEE BY REQUEST OF THE GOVERNOR

Introduced: 3/31/21 Referred: Labor & Commerce, Finance

A BILL

FOR AN ACT ENTITLED

"An Act establishing the Consumer Data Privacy Act; establishing data broker registration requirements; making ~~a~~ certain violations of the Consumer Data Privacy Act an unfair or deceptive trade practice; and providing for an effective date."

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF ALASKA:

*** Section 1.** AS 44.33.020(a) is amended by adding a new paragraph to read:

(45) establish and maintain a data broker registry.

*** Sec. 2.** AS 45 is amended by adding a new chapter to read:

Chapter 49. Consumer Data Privacy Act.
Article 1. Collection, Sale, or Disclosure of Consumer Personal Information.

Sec. 45.49.010. Notice of collection, sale, or disclosure of personal information. (a) A business that collects personal information from a consumer shall notify the consumer at or before collecting the information. Notification to the consumer must indicate the categories of personal information that will be collected, the ~~specific~~ purposes for which each category of personal

information will be used, and the consumer's right to opt out of the sale of the consumer's personal information and use of the consumer's precise geolocation data under AS 45.49.050. A business may not collect an additional category of personal information or use the collected personal information for an additional purpose without first notifying the consumer in accordance with this section.

(b) A business shall maintain, and update at least once every 12 months, in the business's online privacy policies and in any state-specific description of consumers' privacy rights, or on the business's Internet website if the business does not maintain those policies, the following information:

(1) a description of a consumer's rights under this chapter;

(2) all the designated methods of the business by which a consumer can request access to or deletion of information as provided under this chapter;

(3) a list of the categories of consumer personal information that the business collected, sold, or disclosed for a business or commercial purpose in the preceding 12 months, and a designation of that information as collected, sold, or disclosed for a business or commercial purpose; or, if the business did not collect, sell, or disclose any consumer personal information for a business or commercial purpose, a disclosure of that fact;

(4) the categories of sources from which the consumer personal information was collected;

(5) a description of the business or commercial purpose for which each category of consumer personal information was collected, sold, or disclosed;

(6) the categories of third parties to which the business sold or disclosed consumer personal information;

(7) a description of a consumer's right to request specific pieces of the consumer's personal information that the business collected;

(8) a statement that information collected to verify a consumer's disclosure or deletion request shall only be used as provided in AS 45.49.060(d) and (e)(1).

(c) In addition to the requirements of (b) of this section, a business shall include on its Internet website

(1) a clear and conspicuous link to an Internet webpage titled "Do Not Collect or Sell My Personal Information" that enables a consumer to exercise the consumer's rights under this chapter; a business may not require a consumer create an account to access this Internet webpage or to opt out under this section; the link must be included

(A) on the homepage of the business's Internet website;

(B) in the business's online privacy policies if the business has online privacy policies; and

(C) in any state-specific description of consumers' privacy rights; and

(2) a description of a consumer's rights under this chapter.

(d) A business may comply with (c) of this section by including the required content on a separate and additional Internet webpage that is dedicated to state consumers. A business shall include on an Internet webpage dedicated to state consumers the content required under (b) and (c) of this section and reasonably ensure that state consumers are directed to the alternative Internet website.

(e) A business subject to this chapter shall provide training to individuals responsible for handling consumer questions or requests under this chapter, including training in how to direct a consumer to exercise the consumer's rights under this chapter.

Sec. 45.49.015. Personal information; notification upon receipt. (a) When a person receives personal information for a business or commercial purpose that a business originally collected from a consumer, the person shall notify the business that the person possesses the personal information and provide the person's contact information. The person shall provide updated contact information to the business if the person's contact information changes.

(b) A person who receives personal information that a business originally collected from a consumer, and who discloses the personal information to another person for a business or commercial purpose, shall notify the business that originally collected the information not later than 10 days after the disclosure. The notification must include the contact information of the person to whom the personal information was disclosed.

(c) A person who receives personal information that a business originally collected from a consumer shall either deidentify the personal information or maintain the personal information in such a way that the person can readily comply with a disclosure or deletion request under this chapter.

(d) A business that collects or has collected personal information from a consumer shall maintain records of each person to whom the business discloses the personal information. The business shall also maintain all records provided to the business under (a) and (b) of this section.

(e) A person may not disclose personal information that a business collected from a consumer unless the personal information is disclosed in accordance with a contract that requires the recipient to comply with a deletion request issued under this chapter.

Sec. 45.49.020. Right to request disclosure of collected personal information. (a) A consumer may request a business that collects or collected the consumer's personal information disclose to the consumer

(1) the categories and specific pieces of personal information that the business collects or collected within the ~~five years~~ twelve (12) months[1] preceding the date of the request;

(2) the sources from which the business collects or collected each category of personal information; and

(3) the business or commercial purpose for the collection of each category of personal information.

(b) A business shall respond to a verified consumer request under this section as required by AS 45.49.060.

Sec. 45.49.030. Right to request deletion of personal information. (a) A consumer may

[1] Shortened the 5 year "look period" to match the CCPA's 1 year period, which will likely be costly and burdensome for businesses to comply with in a manner that seems likely to outweigh any potential benefits to consumers. To illustrate potential IT systems, technical, business and operational complications, covered businesses that receive verified consumer requests when the ACPA becomes effective on January 1, 2023, which will require identifying, accessing and reviewing personal information back to January 1, 2018 (or when the business exemption (for applicants, employees, etc.) expires on January 1, 2024, which will require identifying, accessing and reviewing personal information back to January 1, 2019). Consider whether the applicable IT systems and personnel and document retention processes are ready for the ACPA and the tremendous amount of financial and human resources it will likely take for companies to seek to comply.

request a business delete any of the consumer's personal information collected by the business from the consumer [within the five years[2]] preceding the date of the request.

(b) Upon receipt of a verified consumer request under this section, a business shall delete the information identified in the request from the business's records.

(c) A business that receives a deletion request under (b) of this section shall direct any service providers and all persons to whom a business disclosed records under AS 45.49.015 to delete the personal information from their records and to provide a written statement verifying that the information has been deleted within 45 days of the consumer's deletion request. A person shall comply with a directive under this subsection. ~~The business shall immediately provide written notification to the attorney general and the consumer of a person who fails to provide written verification of compliance.~~

(d) A person is not required to delete personal information under (c) of this section if the information must be maintained to

(1) complete the transaction for which the personal information was collected;

(2) provide a good or service requested or reasonably anticipated within an ongoing business relationship with the consumer;

(3) fulfill the terms of a written warranty or product recall conducted in accordance with federal law;

(4) perform a contract between the business and consumer;

(5) detect security incidents; protect against malicious, deceptive, fraudulent, or illegal activity; or prosecute those responsible for that activity;

(6) identify and repair errors that impair existing, intended functionality of a product or service;

(7) exercise a right provided for by law, including the right under the First Amendment of the United States Constitution to freedom of expression, or ensure the right of another consumer to exercise that consumer's right to freedom of expression;

(8) comply with a search warrant, subpoena, or court order;

(9) engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws, if

(A) the deletion of information is likely to seriously impair or render impossible the achievement of the research; and

(B) the consumer has provided informed consent to the research;]

(10) enable solely internal uses that are reasonably aligned with the consumer's expectations, based on the consumer's relationship with the business; or

[2] The ACPA states a maximum 5 year look back, which suggests that personal information collected more than 5 years ago would not technically be subject to the erasure request. Whether this type of potential benefit can be realized would seem at least in part dependent upon whether a business' IT systems and other records included information regarding the date of collection. It might be more efficient to simply delete all personal information subject to a verifiable erasure request that is not needed for other purposes subject to exemption from erasure requirements (e.g., to comply with ongoing contractual obligations, etc.).

(11) comply with a legal obligation.

Sec. 45.49.040. Right to request disclosure of personal information sold or disclosed for a business or commercial purpose. (a) A consumer may request that a business that sold or disclosed the consumer's personal information within the last ~~five years~~ twelve (12) months for a business or commercial purpose disclose to the consumer

(1) the third parties subject to AS 45.49.015 in possession of the consumer's personal information;

(2) the categories of personal information or specific pieces of personal information that were sold or disclosed to each third party for a business or commercial purpose;

(3) for the third parties to which the business directly disclosed the consumer's personal information for a business or commercial purpose, the business or commercial purpose for disclosing each category of personal information.

(b) A business shall respond to a verified consumer request under this section as required by AS 45.49.060.

Sec. 45.49.050. Right to opt out or for a minor to opt in. (a) A consumer may, at any time, request that a business not sell the consumer's personal information or not sell particular categories of the consumer's personal information.

(b) A business shall limit the use and disclosure of a consumer's precise geolocation data to that necessary to provide goods or services that a consumer requests and reasonably expects, or goods and services the business reasonably expects the consumer will request. A business may use a consumer's precise geolocation data for other purposes if the consumer consents to the use. A consumer who consents to the use of the consumer's precise geolocation data for other purposes may, at any time, request that the business stop using the data for other purposes. In this subsection, "consents" means the consumer agrees in writing, in an agreement separate from any other user agreement, to the business's use of the consumer's precise geolocation data for other purposes.

(c) A business shall respond to a verified consumer request under this section as required by AS 45.49.060, unless the consumer subsequently provides a clear and explicit renunciation of the request. For one year after receiving a request under (a) or (b) of this section, a business may not contact the consumer to request that the consumer renounce the request.

(d) If a business has actual knowledge that a consumer is under 18 years of age, the business may not disclose the consumer's personal information for a business or commercial purpose, or use the consumer's precise geolocation data for a purpose other than to provide goods or services that the consumers reasonably requests and expects. A business that recklessly disregards a reasonable likelihood that a consumer is under 18 years of age is considered to have actual knowledge of the consumer's age. A parent or guardian with legal custody of a consumer who is at least 13 years[3] of age but under 18 years of age may authorize the sale or disclosure of the consumer's personal information or the use of the consumer's precise geolocation data for any purpose.

(e) A business subject to this section may only use the personal information collected from a consumer's request under this section to comply with the request, unless otherwise authorized by the consumer or by law.

Sec. 45.49.060. Disclosure or deletion request; process. (a) A business shall respond to a

[3] Are children under 13 intentionally being excluded from the option of parental consent?

verified consumer request under AS 45.49.020 or 45.49.040 by ~~(1)~~ providing the requested information electronically to the consumer in a portable and, to the extent technically feasible, readily useable format that allows the consumer to transmit the information to another entity without hindrance.~~;~~

~~(2) if the information provided under (1) of this subsection is not in a human-readable format, providing the requested information to the consumer in a human-readable format; in this paragraph, "human-readable" means a format that is easily readable to the consumer; and~~

~~(3) at the consumer's request, providing the requested information by mail.~~[4]

(b) A business subject to this chapter shall designate at least two methods for a consumer to submit a request under AS 45.49.020 - 45.49.050, including, at a minimum, a toll-free telephone number and an electronic mail address. If a business maintains an Internet website, the website must include an option to submit requests under AS 45.49.020 - 45.49.050 on a public facing page. A designated method for submitting requests may include a mailing address, electronic mail address, Internet website, Internet web portal, toll-free telephone number, other applicable contact information, or any new, consumer-friendly means of contacting a business as determined by regulation.

(c) A person may not charge a consumer a fee for performing a duty required by this chapter.

(d) A person may only use the information provided by a consumer in a request made under AS 45.49.020 - 45.49.050 to identify the consumer and comply with the request.

(e) In response to a request made under AS 45.49.020 - 45.49.050, a business shall

(1) promptly determine whether the request is a verified consumer request as defined in AS 45.49.290; to make a determination under this paragraph, a business

(A) may require reasonable authentication considering the nature of the personal information requested;

(B) may not require that a consumer create an account with the business; however, if the consumer maintains an account with the business, the business may require the consumer submit the request through the account;

(2) identify in writing the personal information subject to a disclosure request; the information disclosed must

(A) encompass the 12-month period preceding the request, or another applicable period designated by the consumer;

(B) be designated by the most relevant category of personal information as defined in AS 45.49.290;

(C) clearly separate information requested under AS 45.49.020 29 and 45.49.040(a)(1) - (3);

(3) disclose and deliver the identified information in a verified disclosure request in writing not later than 45 days after receipt of the request;

(4) not later than 45 days after receipt of a verified deletion request, comply with AS 45.49.030, and provide confirmation of compliance to the consumer.

[4] Delete the requirement that responses to verified consumer requests be made in a "'human-readable'" form as well as by mail (if requested by the consumer), which could result in yet further costs and operational burdens for businesses without obvious benefits to consumers since responses in a "portable" and "readily useable" format (e.g., the CCPA approach) are expected to suffice.

(f) The time to respond to a disclosure or deletion request under (e)(3) and (4) of this section may be extended once for an additional 45 days when reasonably necessary. If the time to respond is extended, the business must notify the consumer of the extension.

(g) A business may disclose or provide confirmation of deletion of information to the consumer by mail, through the consumer's account with the business, or electronically at the consumer's request if the consumer does not have an account with the business.

(h) Notwithstanding any other requirement in this section, if a consumer's requests are manifestly unfounded or excessive, in particular because of the requests' repetitive character, a business may either charge a reasonable fee, taking into account the administrative costs of complying with the consumer's request, or refuse to act on the request. The business shall notify the consumer of a decision to charge a fee or to deny a request within the timeline provided under (f) of this section. The notification must ~~completely~~ reasonably explain the business's reason for finding the request excessive or unfounded, including ~~all~~ pertinent facts[5]. The business shall bear the burden of proving that a consumer's request is manifestly unfounded or excessive.

(i) A business is not required to respond to a disclosure or deletion request under AS 45.49.020 - 45.49.040 if the consumer making the request has made two verified consumer requests in the previous 365 days.

(j) A business is not required under this section to retain personal information collected for a single, one-time transaction, if the business does not sell or disclose the information.

(k) A business is not required under this section to reidentify or otherwise link any data that, in the ordinary course of business, is not maintained in a manner that would be considered personal information.

(*l*) A business is not required to provide or delete information under this section if the business cannot verify the consumer request as provided under (e) of this section.

Sec. 45.49.070. Third-party disclosure of personal information. (a) A third party may not disclose personal information to another person if the personal information was originally collected in violation of AS 45.49.010 or 45.49.050. A third party that reasonably inquires into whether personal information was collected in violation of AS 45.49.010 or 45.49.050, and reasonably concludes that information was not obtained in violation of AS 45.49.010 or 45.49.050 may not be held liable for a violation under this section.

(b) A third party may not disclose a consumer's personal information for a business or commercial purpose unless the third party receives written confirmation from the business that originally collected the personal information that the information was collected in compliance with AS 45.49.010 and 45.49.050.

Sec. 45.49.080 Service provider obligations. (a) A service provider may not

(1) retain, use, or disclose personal information received from a business for any purpose other than to perform the services specified in a written contract with the business;

(2) combine personal information received from a business with personal information the service provider receives from other sources, unless otherwise provided in regulations adopted by the attorney general;

[5] Focus notification obligations on businesses by tightening these provisions based on a reasonableness standard.

(3) disclose personal information received from a business to any other person without first

(A) receiving written consent of the business to disclose the personal information to the other person; and

(B) entering into a written contract with the other person that prohibits the other person from engaging in conduct prohibited under this section.

(b) A person who receives personal information from a service provider may not disclose the personal information to any other person.

Sec. 45.49.090. Exemptions. (a) This chapter does not apply to

(1) 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 in 45 C.F.R. Part 160 and 164, established under the Health Insurance Portability and Accountability Act of 1996 (P.L. 104 - 191) and the Health Information Technology for Economic and Clinical Health Act (P.L. 111 - 5); in this paragraph, "protected health information" has the meaning given in 45 C.F.R. 160.103;

(2) a covered entity governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services in 45 C.F.R. Part 160 and 164, established under the Health Insurance Portability and Accountability Act of 1996 (P.L. 104 - 191), to the extent the provider or covered entity maintains patient information in the same manner as medical information or protected health information as described in (1) of this subsection;

(3) 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, under good clinical practice guidelines issued by the International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use, or human subject protection requirements of the United States Food and Drug Administration;

(4) vehicle or ownership information retained or shared between a new motor vehicle dealer and the motor vehicle manufacturer, if the information is shared for the purpose of or in anticipation of effectuating a vehicle repair covered by a vehicle warranty or recall conducted under 49 U.S.C. 30118 - 30120, provided that the new motor vehicle dealer or vehicle manufacturer does not sell, share, or use the information for any other purpose.

(b) Notwithstanding other provisions of this chapter, a person may disclose a consumer's personal information to

(1) comply with federal, state, or local law;

(2) comply with a civil, criminal, or regulatory inquiry or an investigation, subpoena, or summons by federal, state, or local authorities;

(3) cooperate with law enforcement agencies concerning conduct or activity that the person 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, deidentified or aggregated consumer information.

(c) Notwithstanding other provisions of this chapter, a business may collect or sell a consumer's personal information if the commercial conduct takes place wholly outside the state. For the purpose of this subsection, commercial conduct takes place wholly outside the state if

(1) the business collected the information while the consumer was outside the state; this does not include the storage of personal information, including on a personal device, while the consumer is in the state and collection when the consumer and stored information subsequently leave the state;

(2) no part of the sale of the consumer's personal information occurred in the state; and

(3) no personal information collected while the consumer was in the state was sold.

(d) Excluding the right to file an action for a violation of AS 45.49.120, this chapter does not apply to

(1) an activity that is subject to 15 U.S.C. 1681 (Fair Credit Reporting Act) that involves 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; a furnisher of information, who provides information for use in a consumer report, or by a user of a consumer report, to the extent the information is used as authorized under 15 U.S.C. 1681 (Fair Credit Reporting Act);

(2) personal information collected, processed, sold, or disclosed under 15 U.S.C. 6801 - 6827 (Gramm-Leach-Bliley Act) and related regulations or under 18 U.S.C. 2721 et seq. (Driver's Privacy Protection Act of 1994) and related regulations.

(e) Excluding the requirements of AS 45.49.010(a) and the right to file an action for a violation of AS 45.49.120, information collected by a business is exempt from this chapter until January 1, 2024, if the information

(1) is collected through a person's

(A) job application to the business;

(B) service as an employee, officer, or director of the business;

(C) ownership of the business;

(D) service as a dentist licensed under AS 08.36, physician licensed under AS 08.64, or a psychologist licensed under AS 08.86; or

(E) work as a contractor for the business; and

(2) consists only of

(A) personal information used solely within the context for which it was collected;

(B) emergency contact information used solely for the purpose of having an emergency contact on file; or

(C) personal information retained solely to administer benefits.

(f) Except for AS 45.49.050 and 45.49.120, personal information contained in written or verbal communication or a transaction between a business and a consumer is exempt from this chapter if

(1) the consumer is ~~a natural person~~[6] acting as an employee, owner, director, officer, or contractor of a corporation, limited liability company, partnership, sole proprietorship, nonprofit, other legal entity or government agency; and

(2) the communication or transaction occurs solely within the context of the business's exercising due diligence regarding a product or service, or to receive a product or service from or provide a product or service to ~~the~~ a corporation, limited liability company, partnership, sole proprietorship, nonprofit, other legal entity or government agency.

(g) A requirement under this chapter does not apply if

(1) compliance with the requirement would violate an evidentiary privilege under state law;

(2) the business provides personal information as part of privileged communication to a person covered by an evidentiary privilege;

(3) the right or obligation would adversely affect a right of another consumer;

(4) the right or obligation would infringe on the noncommercial activity of a person or entity exercising rights under art. I, sec. 5, Constitution of the State of Alaska.

(h) If a series of steps or transactions are component parts of a single transaction, intended from the beginning to avoid the reach of this chapter, including a business's disclosure of information to a third party to avoid the definition of "sell" in AS 45.49.290, the steps or transactions may not be considered separate for the purposes of determining compliance with, an exception to, or a violation of this chapter.

(i) In this section,

(1) "contractor" means a person who is not an employee of a business but provides a service to the business under a written contract;

(2) "director" has the meaning given in AS 10.06.990;

(3) "motor vehicle manufacturer" means a person that meets the definition of "motor vehicle manufacturer" in AS 21.59.290 or the definition of "manufacturer" in AS 45.25.990;

(4) "new motor vehicle dealer" has the meaning given in 16 AS 45.25.990;

(5) "officer" means a person appointed or designated as an officer of a corporation by or under applicable law or the corporation's articles of incorporation or bylaws, or a person who performs for the corporation the functions usually performed by an officer of a corporation;

(6) "owner" means an individual who

(A) owns, directly or indirectly, or has the power to vote more than 50 percent of the outstanding shares of any class of voting security of a business;

(B) controls, in any manner, the election of a majority of the directors or of individuals exercising similar functions; or

(C) has the power to exercise a controlling influence over the majority of the

[6] Moved to definition of "consumer".

directors or of individuals exercising similar functions;

(7) "ownership information" means the name of each registered owner and accompanying contact information;

(8) "vehicle information" means the vehicle identification number; the vehicle's make, model, or year; or the vehicle's odometer reading.

Article 2. Activities and Penalties Relating to Personal Information.

Sec. 45.49.100. Retaliation prohibited. (a) A business may not retaliate against a consumer in response to a consumer exercising rights under this chapter. Retaliation includes

(1) denying goods or services;

(2) charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties;

(3) providing a different level or quality of goods or services to a consumer;

(4) suggesting that a consumer will receive a different price or rate for goods or services, or a different level or quality of goods or services.

(b) Notwithstanding (a) of this section, a business may charge a consumer a different rate or provide a different level or quality of goods or services to a consumer if the difference is reasonably related to the value provided to the business by the consumer's data.

(c) A business may offer a consumer a financial incentive for the collection, sale, or retention of personal information, including direct payments to a consumer as compensation. A business may also offer a different price, rate, level, or quality of goods or services to the consumer if the price or difference is directly related to the value provided to the business by the consumer's data. A business that offers a financial incentive under this subsection

(1) shall notify consumers of the financial incentives;

(2) shall obtain a consumer's consent before entering a consumer into a financial incentive program; to obtain a consumer's consent under this paragraph, the business shall provide the consumer access to a clear description of the material terms of the financial incentive program; the consumer may revoke consent at any time;

(3) may not use financial incentive practices that are unjust, unreasonable, coercive, or usurious.

Sec. 45.49.110. Transfer of information in a merger or acquisition. A business may transfer (or share on a confidential basis on the condition that any recipients are contractually bound to confidentiality and non-use obligations for any purpose other than evaluating and consummating a proposed transaction of the type listed under this section)[7] a consumer's personal information to a third party ~~as part of~~ in connection with a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the business. If the third party decides to change how it uses or shares the consumer's personal information in a manner that is materially inconsistent with the promises made at the time of collection, the third party shall notify the consumer before the change. The notice must ensure that existing consumers can easily exercise consumers' rights under this chapter. A transfer does not authorize a business to make material, retroactive privacy policy changes or other

[7] Revisions were added to avoid ambiguity regarding whether the parties to a contemplated M&A deal are able to share personal information prior to closing (e.g., human resources related data to facilitate seamless integration post-closing).

changes in a manner that violates state law.

Sec. 45.49.120. Duty to maintain reasonable security measures. A business that owns, licenses, or maintains a consumer's personal information shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.[8]

[8] Suggest that the Attorney General provide regulatory guidance (e.g., through AG reports or regulations) to clarify the meaning of "reasonable security procedures and practices" such as by establishing a minimum baseline for "reasonable security" procedures (see the California AG's 2016 Data Breach Report (https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf) citing the Center for Internet Security's 20 Critical Security Controls (CIS Controls (cisecurity.org)). Alternatively, update sec. 45.49.120.

Sec. 45.49.130. Violations. (a) A violation of Sec. 45.50.120 ~~this chapter~~ resulting in the unauthorized access and exfiltration, theft or disclosure of non-encrypted and non-redacted sensitive personal information[9] is an unfair or deceptive act or practice under AS 45.50.471 - 45.50.561.

~~(b) In an action brought under AS 45.50.531(a), a consumer whose personal information is subjected to unauthorized access, destruction, use, modification, or disclosure has suffered an ascertainable loss of $1 or of an amount proven at trial, whichever is greater.~~[10]

[9] Updated sec. 45.49.130 to clarify that breaches of sec. 45.49.120 apply only to nonencrypted and nonredacted "sensitive personal information" for purposes of sec. 45.49.130 since we anticipate that it would be extremely costly and burdensome for claims to based on a definition of personal information that is broader even than under the California CCPA.

[10] **Delete the automatic $1 damages and private right of action provisions (Sec. 45.49.30(b))** including because not all data breaches are necessarily the result of "unfair and deceptive trade practices" or result in harm to individuals. In our experience responding to numerous data incidents/breaches:

1) key questions have included whether there has actually been unauthorized access to personal information and if so 2) whether there has been any harm to individuals;

2) in multiple scenarios, a breached company has concluded (reasonably and correctly in the view of in-house and outside counsel obligated to indicate otherwise if the facts so warranted under ethical rules and obligations) that there has been no harm to individuals (see Sec. 45.48.010(c) (Disclosure of breach of security): **"…**disclosure is not required if, after an appropriate investigation and after written notification to the attorney general of this state, the covered person determines that there is **not a reasonable likelihood that harm to the consumers whose personal information has been acquired has resulted or will result from the breach**" (emphasis added));

3) the marks of a diligent, trustworthy and reasonable company that has experienced a breach tend to be measured based on their level of responsiveness, expediency, transparency/timeliness of communication with impacted individuals and execution of effective/timely root cause analyses and remediation measures to identify and plug any holes and implement better processes, procedures and technical measures going forward;

4) the sophistication of hackers, cyber criminals and "bad actor" nation states is increasing along with exponentially increasing volumes of "attack surfaces" (i.e., proliferating devices, cloud/SaaS services, internet-of-things devices, software applications, etc.) to perpetrate data breaches through;

5) the reality is that even well intended companies that are trying to do (and are actually doing) the right things with reasonable security measures are still getting hacked/breached;

6) even for high profile cases where the FTC has done deep dives on data breaches, our understanding is that the FTC has not always concluded that the company that experienced the data breach engaged in unfair and deceptive trade practices; and

7) **for companies that have taken reasonable steps to prevent and respond to data breaches --and are also not even involved with "selling" personal information (including Business-to-Business focused companies)-- it would be particularly punitive/onerous to impose legislated damages (e.g., $1) even if here was no harm to consumers**.

Note also that deleting the private right of action is consistent with the approach under the VCDPA.

Delete the reference to AS45.50.531(a) (with its reference to damages of the greater of 3X actual damages or $500):

- to summarize the essence of the points above, not all data breaches are created equal so it would not be fair or reasonable to subject companies that are not selling personal information, not engaged in "high risk" business models and that have made diligent efforts to seek to prevent and respond to data breaches to the type of plaintiff's class action bar "feeding frenzy" that could result if the references related to AS45.50.531(a) and the automatic $1 damages provision under Sec. 45.49.30(b) are not deleted;

(c) Actions pursuant to this section may be brought by the Attorney General if, prior to initiating any action against a business, the Attorney General provides a business 30 days' written notice identifying the specific provisions of this section the Attorney General alleges have been or are being violated. In the event a cure is possible, if within the 30 days the business actually cures the noticed violation and provides the Attorney General an express written statement that the violations have been cured and that no further violations shall occur, no action for damages may be initiated against the business. Notwithstanding the foregoing, the Attorney General shall not be required to provide a business 30 days' written notice for repeat violations of the same specific provisions of this section for a violation involving a substantially similar or analogous factual scenario where the Attorney General previously provided the business 30 days' written notice for the prior violation.[11]

(d) A person who violates this chapter commits the greater of

(1) one violation for each action or omission that violates this chapter;

(2) one violation for each person the violation affects; or

(3) one violation for each day the violation continues.

(d) The legislature may appropriate funds recovered as a result of an action brought under this section to the consumer privacy account established in AS 45.49.140. The Department of Law may use money in the account, without further appropriation, to offset costs incurred by the department in connection with enforcing this chapter.

Sec. 45.49.140. Consumer privacy account. The consumer privacy account is established in the general fund. The legislature may appropriate funds to the consumer privacy account from any civil penalty collected in an action brought by the attorney general under this chapter.

Article 3. Data Broker Registry.

- hundreds of value-destroying (and even bankruptcy inducing) class action law suits have resulted from overly broad privacy legislation even in the absence of clear harm (e.g., the Illinois Biometric Information Privacy Act ("**BIPA**"));
- In March 2021, Illinois House Minority Leader Jim Durkin stated that damages awards under BIPA can be "enough to put any small business into insolvency" (Illinois Legislature Considers Employer-Friendly Change to BIPA Liability (winston.com)); and
- We trust the Governor would not support BIPA-type plaintiff's class action feeding frenzy risks for Alaska.

[11] Include Cure Provisions (in addition to deleting the automatic $1 damages and private right of action provisions and deleting the reference to AS45.50.531(a) as suggested above) providing that:

- Before initiating an action for a ACPA violation, the AG must give the offending business, service provider, or other person notice of the alleged violation and at least 30 days to cure it;
- If the business does not (or cannot) cure the violations, the AG could then seek specified civil penalties (e.g., Cal. Civ. Code sec. 1798.155(b)); and
- To address AG office concerns about potential circumvention and abuse of the policy and purpose underling the cure provision, please see the last sentence providing an exception stating that the cure period provision does not apply to serial offenders that repeatedly commit the same violations.

See also the cure period under VCPA § 59.1-580(B).

If provisions enabling a private right of action are not deleted, we suggest updating the bullet points above to state that both plaintiffs and the AG would need to provide a cure period.

Sec. 45.49.200. Data broker registration. (a) On or before January 31 following each year that a business meets the definition of data broker in AS 45.49.290, the business shall register with the commissioner of commerce, community, and economic development in accordance with this section.

(b) The data broker shall provide, on a form provided by the commissioner, the following information:

(1) the name of the data broker;

(2) the data broker's primary physical and mailing addresses;

(3) the data broker's electronic mail address;

(4) the data broker's primary Internet website address; and

(5) the data broker's "Do Not Collect or Sell My Personal Information"

Internet website address as required under AS 45.49.010(c) or alternative Internet webpage that meets the requirements of AS 45.49.010(d).

(c) The data broker shall pay a registration fee in an amount established by the department in regulation.

Sec. 45.49.210. Data broker registry publicly displayed. The commissioner of commerce, community, and economic development shall make the information provided by data brokers available on the department's Internet website.

Article 4. Miscellaneous Provisions.

Sec. 45.49.250. Regulations. (a) The attorney general, in accordance with AS 44.62 (Administrative Procedure Act), shall on or before [INSERT MONTH, 2021] solicit broad public participation[12] and adopt regulations that

(1) create specific exceptions required to comply with state or federal law;

(2) govern the Internet webpage requirement of AS 45.49.010, including

(A) the use of a recognizable and uniform mark to identify the opportunity to exercise a right under this chapter;

(B) the submission of a consumer request;

(C) a business's compliance with a request under AS 45.49.050;

(3) update, as necessary, additional categories of personal information required to be disclosed in response to relevant changes in technology, data collection practices, privacy concerns, or obstacles to implementation;

(4) update, as necessary, the interpretation of unique identifiers in response to relevant changes in technology, data collection practices, privacy concerns, or obstacles to implementation update, as necessary, additional categories of personal information required to be disclosed in response to relevant changes in technology, data collection practices, privacy concerns, or obstacles to implementation;

(5) update, as necessary, the interpretation of designated methods for submitting requests to facilitate a consumer's ability to obtain information from a business;

[12] We suggest inviting public participation (e.g., the California AG's Office held seven public forums and received 300+ written comments during its CCPA rulemaking activities).

(6) establish requirements to ensure that notices and information provided under AS 45.49.010 are in plain language, accessible to consumers with disabilities, and available in the language primarily used by the business to interact with the consumer, including with regard to financial incentive offerings;

(7) govern the process by which a business verifies a consumer request under AS 45.49.020 - 45.49.060, in a manner intended to minimize the administrative burden on the consumer and taking into account the available technology, security concerns, and the burden on the business;

(8) designate the process for a consumer to authorize a representative to exercise the rights provided under this chapter on the consumer's behalf.

(b) The attorney general may adopt regulations that

(1) establish rules and procedures for processing and complying with a verified consumer request for specific pieces of personal information relating to a household to address obstacles to implementation and privacy concerns;

(2) state that service providers may combine personal information for specified purposes;

(3) are necessary to further the purpose of this chapter.

(d) The Attorney General shall not bring an enforcement action under this title until six months after the publication of the final regulations issued pursuant to this section or [INSERT MONTH, 2023], whichever is sooner.

Sec. 45.49.260. Provisions not waivable. A consumer's waiver of the provisions of this chapter is contrary to public policy and is unenforceable and void. This section does not prevent a consumer from

(1) declining to request information from a business;

(2) declining to opt out of a business's collection, sale, or disclosure of the consumer's personal information; or

(3) authorizing a business to sell the consumer's personal information after previously opting out.

Sec. 45.49.270. Liberal construction. The intent of this chapter is remedial and its provisions shall be liberally construed.

Article 5. General Provisions.

Sec. 45.49.290. Definitions. In this chapter, unless the context indicates otherwise,

(1) "aggregated consumer information" means information that relates to a group or category of consumers from which individual consumer identities have been removed, and that is not linked or reasonably linkable, including by a device, to any consumer or household; "aggregated consumer information" does not include one or more individual consumer records that have been deidentified;

(2) "business" means a sole proprietorship, partnership, limited liability company, corporation,

association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners ("For profit entity" or "For-profit entities"), and collects or has collected consumers' personal information, or on the behalf of which that information is collected, alone or jointly with others, determines the purposes and means of processing consumers' personal information; to meet the definition of "business" in this paragraph, the entity must do business in the state and

(A) satisfy one or more of the following thresholds:

~~(i) had annual gross revenues of $25,000,000 or more in the year 2022 or in any year thereafter;~~[13]

(i~~i~~) in the most recent completed calendar year, alone or in combination, bought or disclosed the personal information of 100,000[14] or more consumers~~persons~~[15] or households;

(ii~~i~~) sold the personal information of a consumer or~~,~~ household~~, or device~~[16] in the last 365 days; or

(B) control or be controlled by a business that meets a threshold in (A) of this paragraph and share common branding, such as a shared name, service mark, or trademark, with the business; in this subparagraph, control is shown if a business has

(i) ownership or the power to vote more than 50 percent of the outstanding shares of any class of voting security of a business;

(ii) control, in any manner, of the election of a majority of the directors or of individuals exercising similar functions; or

(iii) the power to exercise a controlling influence over the majority of the directors or of individuals exercising similar functions;

Notwithstanding any provision to the contrary above, the definition of "business" excludes For-profit entities that:

(a) primarily conduct business as service providers ("Business Vendor(s)") to customers that are For-profit entities ("Business Customer(s)");

(b) solely use personal information received from Business Customers for the purpose or providing

[13] Follow the approach under the Virginia Consumer Data Protection Act ("VCDPA") of refraining from including a standalone revenue threshold for determining applicability by deleting 2(A)(i). A volume of personal data-based threshold logically makes more sense than a revenue-based approach (e.g., a small social media, e-commerce other Internet company without significant (or any) revenue could be processing far more personal information than even large B2B companies generating $5B+ in revenue).

(Alternatively, increase the annual gross revenue threshold to $5B (subject to automatic increases based on the CPI index) (i.e., $25M is too low and would catch a lot of Business-to-Business focused companies that are not the target of the ACPA and are not engaged in high risk business models related to personal information) as follows: "had annual gross revenues of $**5,000,000,000 (adjusted automatically to reflect any increase in the Consumer Price Index in each year after the year 2022 effective as January 1 of such year)** or more in the year 2022 or in any year thereafter" (bold supplied for suggested updates.)

[14] Consider increasing the threshold to exempt more small and midsize businesses that do not sell personal data.

[15] Update to align with the defined terms under the ACPA (e.g., "consumer").

[16] Follow the approach under the CPRA, which deleted the CCPA reference to "device" when increasing the volume of consumers and households threshold from 50,000 to 100,000.

services to such Business Customers (provided that the applicable contract between the applicable Business Vendor and Business Customer prohibits the Business Vendor receiving personal information from retaining, using or disclosing such personal information for any purpose other than for the specific purpose of performing the services specified in the applicable contract);

(c) do not determine the purposes of processing (excluding the purpose of providing services to Business Customers per their request as part of the Business Vendor's business model or revenue generation activities); and

(d) do not sell personal information received from Business Customers (the "Business-to-Business Exemption")[17].

(3) "business purpose" means a use for an operational or other notified purpose that is either reasonably necessary and proportionate to achieving the operational purpose for which personal information was collected or processed, or in a compatible context; "compatible context" includes

(A) auditing related to a current interaction with the consumer and concurrent transactions, including counting ad impressions to unique visitors, verifying positioning and quality of ad impressions, and auditing compliance with this specification and other standards;

(B) detecting security incidents, protecting against malicious, deceptive, fraudulent, or illegal activity, and prosecuting those responsible for that activity;

(C) debugging to identify and repair errors that impair existing intended functionality;

(D) short-term, transient use, provided that the personal information is not disclosed to another third party and is not used to build a profile about a consumer or alter an individual consumer's experience outside the current interaction, including the contextual customization of ads shown as part of the same interaction;

(E) performing services on behalf of the business or service provider, including maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing financing, providing advertising or marketing services, providing analytic services, or providing similar services on behalf of the business or service provider;

(F) conducting internal research for technological development and demonstration;

(G) performing activities to verify or maintain the quality or safety of a service or device that is owned, manufactured, manufactured for, or controlled by the business, and to improve, upgrade, or enhance the service or device;

(4) "categories of personal information" includes any of the enumerated categories of personal information as defined in this section, any categories of personal information identified by a regulation adopted under this chapter, and any additional categories of personal information not specifically enumerated;

(5) "categories of sources" includes the consumer, advertising networks, Internet service providers, data analytics providers, government entities, operating systems and platforms, social networks, data brokers, other sources listed in regulations adopted under this chapter; and other types or groupings of persons or entities from which a business collects personal information about consumers,

[17] Suggest exempting companies (including Business-to-Business companies) that are not "selling" personal information (but rather that are just using the customer's personal information to perform services for the same customer). See the VCDPA approach of carving out of the definition of "consumers" any individuals acting in a business-to-business/commercial or employment context.

described with enough particularity to provide consumers with a meaningful understanding of the type of person or entity;

(6) "categories of third parties" includes advertising networks, internet service providers, data analytics providers, government entities, operating systems and platforms, social networks, data brokers, other sources listed in regulations adopted under this chapter; and other 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;

(7) "collect" includes buying, renting, gathering, obtaining, receiving, or accessing any personal information pertaining to a consumer by any means, actively or passively receiving information from the consumer, or by observing the consumer's behavior;

(8) "commercial purpose" includes marketing, advertising, and any other purpose that advances a person's commercial or economic interests; "commercial purpose" does not include the purpose of engaging in speech that state or federal courts have recognized as noncommercial speech, including political speech and journalism;

(9) "consumer" means a natural person who is a resident of the state, however identified, including by any unique identifier, who is physically present in the state with the intent to remain indefinitely in the state under the requirements of AS 01.10.055 but does not include a natural person acting in a commercial (business-to-business) or employment context such as an employee, owner, director, officer, or contractor of a corporation, limited liability company, partnership, sole proprietorship, nonprofit, other legal entity or government agency[18];

(10) "data broker" means a business as defined in (2) of this section that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship; "data broker" does not include a consumer reporting agency to the extent the agency is covered by 15 U.S.C. 1681 et seq. (Fair Credit Reporting Act) or a financial institution to the extent the institution it is covered by the Gramm-Leach-Bliley Act (P.L. 106 - 102) and implementing regulations;

(11) [["disclose"[19] ~~includes all~~ means forms of disclosure (excluding for purpose of serving as a service provider or under the Business-to-Business Exemption)~~, including the disclosure~~ of personal information related to a sale of personal information];

(12) "deidentified" means that the information cannot reasonably identify, relate to, describe, be capable of being associate with, or be directly or indirectly linked to an individual consumer, and the business

(A) has implemented technical safeguards that prohibit reidentification of the consumer to whom the information may pertain;

(B) has implemented business processes that specifically prohibit reidentification of the information;

(C) has implemented business processes to prevent inadvertent release of deidentified information; and

[18] Follow the VCDPA approach of providing for a general exemption from the definition of "consumers" for any individuals acting in a commercial (i.e., business-to-business) or employment context.

[19] The initial draft reference to "all forms of disclosure" looks overly broad. Suggest either (a) deleting the definition of "disclose" entirely as unnecessary especially given that the definition of "sale" includes a reference to "disclosing" (noting too that the CCPA does not include a definition of "disclose") or (b) incorporating the proposed revisions.

(D) makes no attempt to reidentify the information;

(13) "device" includes a computer and physical object that can

(A) read, write, or store information that is represented in numerical form;

(B) connect to the Internet, directly or indirectly, or to another device;

(14) "homepage" means

(A) the introductory page of an Internet website where personal information is collected;

(B) in the case of a mobile application, "homepage" means the application's platform page or download page, a link within the application, and any other location that allows consumers to review the notice required by 6 AS 45.49.010;

(15) "Internet webpage" means a document accessible through the Internet with a unique universal resource locator (URL) code;

(16) "person" means a natural person, sole proprietorship, corporation, limited liability company, partnership, firm, association, and any other legal entity or non-governmental organization or group of persons acting in concert;

(17) "personal information"

(A) means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household; in this subparagraph, "information that identifies" includes

(i) a real name, alias, postal address, unique personal identifier, online identifier, Internet protocol address, electronic mail address, account name, social security number, driver's license number, or passport number;

(ii) characteristics of protected classifications under state or federal law; (iii) any category of personal information as defined in 24 AS 45.48.090;

(iv) commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies;

(v) biometric information, which includes (excluding data points and mathematical representations based on biometric data) an individual's physiological, biological, or behavioral characteristics; deoxyribonucleic acid, that can be used, singly or in combination with other identifying data, to establish individual identity; imagery of the retina, fingerprints, face, vein patterns, or voice recordings that can be used as an identifier template; keystroke patterns or rhythms; or sleep, health, or exercise data;

(vi) Internet or other electronic network activity information, including browsing history, search history, and information regarding a consumer's interaction with an Internet website, application, or advertisement;

(vii) geolocation data, including precise geolocation data;

(viii) audio, electronic, visual, thermal, olfactory, or similar information;

(ix) professional or employment information;

(x) education information that is not publicly available, personally identifiable

information as defined in 20 U.S.C. 1232g; 34 C.F.R. Part 99 (Family Educational Rights and Privacy Act);

(xi) inferences drawn from any of the information identified in this subparagraph to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes;

(B) does not include publicly available information that is lawfully made available from federal, state, or local government records; biometric information as described in (A) of this paragraph, collected by a business without a consumer's knowledge is not considered publicly available information;

(C) does not include consumer information that is deidentified or aggregated;

(18) "processing" means any operation or set of operations performed on personal data or on sets of personal data, whether or not by automated means;

(19) "precise geolocation data" means any data that is derived from a device that is used or intended to be used to locate a consumer within a geographic area that is equal to or less than the area of a circle with a radius of 1,850 feet, except as otherwise provided in regulations adopted under this chapter;

(20) "research" means scientific, systematic study and observation that is in the public interest and that adheres to all other applicable ethics and privacy laws or studies conducted in the public interest and is

(A) compatible with the business purpose for which the personal information was collected;

(B) subsequently pseudonymized and deidentified, or deidentified and in the aggregate, such that the information cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer; personal information is considered pseudonymized if the information is processed so that it is no longer attributable to a specific consumer without the use of additional information, and the additional information is kept separately and is subject to technical and organizational measures to ensure that the personal information is not attributed to an identified or identifiable consumer;

(C) subject to technical safeguards that prohibit reidentification of the consumer to whom the information may pertain;

(D) subject to business processes that specifically prohibit reidentification of the information;

(E) subject to business processes to prevent inadvertent release of deidentified information;

(F) protected from any reidentification attempts;

(G) used solely for research purposes that are compatible with the context in which the personal information was collected;

(H) not used for a commercial purpose; and

(I) subjected by the business conducting the research to additional security controls that limit access to the research data to individuals in the business as necessary to carry out the research purpose;

(21) "sale," "sell," or "sold" means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other

means, a consumer's personal information by the business to another business or a third party for monetary or other valuable consideration; "sale," "sell," or "sold" does not include

(A) a consumer using or directing a business to intentionally disclose personal information or using the business to intentionally interact with a third party[20], provided the third party does not also sell the personal information, unless that disclosure would be consistent with the provisions of this title; a consumer is not acting intentionally when hovering over, muting, pausing, or closing a given piece or content;

(B) a business's using or sharing an identifier for a consumer who has opted out of the sale of the consumer's personal information for the purpose of alerting third parties that the consumer has opted out;

(C) a business's using or sharing with a service provider a consumer's personal information that is necessary to perform a business purpose if

(i) the business has provided notice of the information being used or shared in its terms and conditions consistent with 18 AS 45.49.010; and

(ii) the service provider does not further collect, sell, or use the consumer's personal information, except as necessary to perform the business purpose;

(D) a business transferring (or sharing on a confidential basis on the condition that any recipients are contractually bound to confidentiality and non-use obligations for any purpose other than evaluating and consummating a proposed transaction of the type listed under this definition) a consumer's personal information as an asset in connection with a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the business, provided that information is used or shared consistent with AS 45.49.020 and 45.49.040; and

(E) personal information disclosed, received or used under the Business-to-Business Exemption;

[20] Consider restating to incorporate the approach under the VCDPA, which provides that "'Sale of personal data' does not include…2. The disclosure of personal data to a third party for purposes of providing a product or service requested by the consumer…."

(22) "sensitive personal information" means:

(a) an individual's first name (or first initial) and last name in combination with one of the following:

(1) Social security number or other tax identification number;
(2) Driver's license number, passport number, military identification number or other unique identification number issued on a government document commonly used to verify the identity of a specific natural person;
(3) Account number, credit or debit card number, in combination with the security or access code, password, or other information required to access the account;
(4) Medical information;
(5) Health insurance information; or
(6) Unique biometric data (excluding data points and mathematical representations based on biometric data) generated from measurements or technical analysis of human body characteristics used to authenticate a specific individual, such as a fingerprint, facial scan (excluding photographs not used or stored for facial recognition purposes), retina or iris image; and

(b) a username or email address in combination with a password or security question and answer that permits access to an [21] account.

(2~~2~~3) "service provider" means a person that receives personal information from a business to be used solely for a business purpose, under a written contract that requires the service provider to comply with AS 45.49.080~~;~~ and on the express condition that any written contract with the service provider shall prohibit the service provider from receiving the information from retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract for the business (or as otherwise permitted by this chapter), including retaining, using, or disclosing the personal information for a commercial purpose other than providing the services specified in the contract with the business[22];

(2~~3~~4) "third party" means any person, except

(A) the business that collected the personal information from the consumer; and

(B) a service provider contracting with the business that collected the personal information from the consumer;

(25) "unique identifier" or "unique personal identifier" includes a device identifier; an Internet protocol address; cookies, beacons, pixel tags, mobile ad identifiers, or similar technology; customer number, unique pseudonym, or user alias; telephone numbers, or other forms of persistent or probabilistic identifiers that can be used to identify a particular consumer or device; or other persistent identifier that can be used to recognize a consumer, a household, or a device that is linked to a consumer or household, over time and across different services; in this paragraph, "probabilistic identifier" means the identification of a consumer or a device to a degree of certainty of more probable than not based on any categories of personal information included in, or similar to, the categories of personal information as defined in this section;

(2~~4~~6) "verified consumer request" means a request that is made by a consumer, by a parent or legal guardian with legal custody of the consumer, or by a natural person or a person registered with the

[21] Deleted previous reference to "online" before "account".
[22] Clarify provisions related to requirements to ensure that service providers comply with use restrictions (e.g., Cal. Civ. Code sec. 1798.140(v)).

United States Secretary of State, authorized by the consumer to act on the consumer's behalf, and that the business can reasonably verify, in accordance with regulations adopted under this chapter, to be the consumer about whom the business has collected personal information.

Sec. 45.49.295. Short title. This chapter may be cited as the Consumer Data Privacy Act.

*** Sec. 3.** AS 45.50.471(b) is amended by adding a new paragraph to read:

(58) violating AS 45.49 (Consumer Data Privacy Act).

*** Sec. 4.** The uncodified law of the State of Alaska is amended by adding a new section to read:

TRANSITION: REGULATIONS. The Department of Law and the Department of Commerce, Community, and Economic Development may adopt regulations necessary to implement the changes made by this Act. The regulations take effect under AS 44.62 (Administrative Procedure Act), but not before the effective date of the law implemented by the regulation.

*** Sec. 5.** Section 4 of this Act takes effect immediately under AS 01.10.070(c).

*** Sec. 6.** Except as provided in sec. 5 of this Act, this Act takes effect January 1, 2023.