



California Consumer Privacy Act of 2018 (CCPA)
Compliance Handbook
Second Edition

By
Arent Fox LLP



IMPORTANT NOTICES

Purpose of the Handbook. The California Consumer Privacy Act of 2018 (CCPA) will take effect on January 1, 2020. CNCDA wants to ensure that its members and the automotive sector generally are prepared for this more stringent set of consumer data privacy regulations. For that reason, CNCDA engaged Arent Fox to prepare this CCPA Compliance Handbook (the “Handbook”). The first section of the Handbook will explain the general requirements of the CCPA. The balance of the Handbook addresses the detailed requirements and implementation procedures that your dealership will need to comply with the new law. The last section of the Handbook includes sample documents to be provided to customers and vendors or to be used internally to aid in your compliance efforts.

Pending Regulations and Ballot Initiative. Since the publication of the first edition of this CCPA Handbook, several amendments to the CCPA have been passed and signed into law. In addition, the Attorney General has published proposed regulations. This second edition incorporates the amendments and the proposed regulations. However, it is our understanding that the Attorney General’s proposed regulations will likely be amended before final regulations are published. In other words, **imminent future changes to the law may impact the compliance information contained in this manual.** Also, on September 25, 2019, Californians for Consumer Privacy filed a new ballot measure called the California Privacy Rights and Enforcement Act (“CCPA 2.0”). If enough signatures are gathered and if this measure passes in November 2020, the CCPA will be further expanded. CNCDA and Arent Fox are monitoring these developments and will issue updated information as appropriate. Contact your counsel and/or the CNCDA legal hotline (916-441-2599) for the most current information.

Electronic Copy of the Handbook. An electronic copy of this Handbook is available to download at CNCDA.org.

Not Intended as Legal Advice. This Handbook is not intended as legal advice or a substitute for legal advice. Instead, it is intended as a source of guidance to California vehicle dealers on the CCPA. The law is subject to constant change and there may have been developments since the date of this publication (December 23, 2019). Readers that require legal advice should contact competent counsel.

Copyright. Copyright © 2019 Arent Fox LLP and California New Car Dealers Association. All rights reserved. Printed in the United States. No part of this Handbook may be reproduced or distributed in any form or by any means without prior written permission from the copyright holders. No claim to official U.S. Government works.

Table of Contents

I.	Summary of the CCPA	4
II.	Determining Whether Your Dealership “Sells” Personal Information.....	9
III.	Data Mapping	12
IV.	CCPA Notice at Collection of Personal Information	13
V.	Privacy Policy	17
VI.	Guidance on Handling Data Subject Access Requests (DSARs)	27
VII.	Guidance on Data Retention Policies	40
A.	<i>Elements of a Data Retention Policy</i>	<i>40</i>
B.	<i>Data Retention Schedule</i>	<i>43</i>
VIII.	Guidance on Data Security	46
IX.	Template CCPA Compliance Checklist for Vendors	49
X.	Data Processing Addendums for Vendor Agreements	50
XI.	Incident Response Manuals	55
XII.	Guidance on Cyber Liability Insurance	56
XIII.	Intersection of the CCPA and California Franchise Law	59
XIV.	Sample Documents	60
A.	<i>Sample Notice at Collection of Personal Information</i>	<i>61</i>
B.	<i>Sample Notice at Collection of Personal Information – Job Applicants and Employees</i>	<i>62</i>
C.	<i>Sample Privacy Policy</i>	<i>63</i>
D.	<i>Sample Privacy Notice</i>	<i>76</i>
E.	<i>Sample In-Person Data Request Form.....</i>	<i>78</i>
F.	<i>Sample Initial Response to Data Request.....</i>	<i>79</i>
G.	<i>Sample Responses to Deletion Requests</i>	<i>80</i>
H.	<i>Sample Responses to Right to Know Requests.....</i>	<i>86</i>
I.	<i>Sample Data Retention Policy</i>	<i>99</i>
J.	<i>CIS Critical Security Controls for Effective Cyber Defense Checklist</i>	<i>102</i>
K.	<i>Sample Data Processing Agreement</i>	<i>104</i>
L.	<i>Short Form Service Provider Agreement Regarding Compliance With CCPA.....</i>	<i>108</i>
M.	<i>Sample Incident Response Manual</i>	<i>109</i>

I. Summary of the CCPA

On June 28, 2018, California became the first U.S. state to enact a comprehensive consumer privacy law with the California Consumer Privacy Act of 2018. The CCPA, which becomes effective on January 1, 2020, grants California residents new rights regarding their personal information and imposes various data protection duties on certain “businesses,” as defined below, conducting business in California.

Covered Businesses

Under the CCPA, a “business” is an entity that: (1) handles “personal information” about California residents; (2) alone, or jointly with others, determines the purposes and means of processing that “personal information”; and (3) does business in California. Most of the CCPA’s obligations apply directly to businesses that meet one of the following threshold requirements: (a) has annual gross revenues in excess of \$25 million; (b) annually buys, receives for its commercial purposes, sells, or shares for commercial purposes personal information regarding at least 50,000 consumers, households, or devices; or (c) derives 50% or more of its annual revenue from selling personal information.¹ In the context of car dealerships, this means that a family of dealerships may be viewed as one business.

Personal Information

“Personal information” is broadly defined as any “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.”² Consumers are natural persons who are California residents.³ Personal information includes, but is not limited to, the following eleven “categories” of information⁴:

1. Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier IP address, email address, account name, social security number, driver’s license number, state identification card number, passport number, or other similar identifiers.
2. Any categories of personal information described in subdivision (e) of [Section 1798.80](#). These include the following items that may apply to vehicle sales or service transactions: signature, physical characteristics or description (such as information included on a driver’s license or other form of identification), telephone number, insurance policy

¹ [Civil Code Section 1798.140\(c\)](#).

² [Civil Code Section 1798.140\(o\)\(1\)](#).

³ [Civil Code § 1798.140\(g\)](#)

⁴ As explained in Section V, these categories of personal information should be listed in your privacy policy. The sample privacy policy in Section XIV(C) contains the categories of personal information that would most likely be collected by car dealerships, but when drafting a specific privacy policy, please confirm all categories of personal information that are collected are included.

number, bank account number (e.g., photocopy of a check), credit card number, debit card number, or any other financial information.

3. Characteristics of protected classifications under California or federal law (e.g. age, gender, race, color, national origin, citizenship, immigration status, primary language, or military status)
4. Commercial information, including records of personal property, products, or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.
5. Biometric information (e.g., thumbprint form).
6. Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer’s interaction with an Internet website, application, or advertisement.
7. Geolocation data (e.g., tracking information that may be collected from a vehicle or from an IP address).
8. Audio, electronic, visual, thermal, olfactory, or similar information.
9. Professional or employment-related information.
10. Education information.
11. Inferences drawn from information collected about a consumer to create a profile reflecting the consumer’s preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, or aptitudes.

The CCPA excludes from the definition of personal information (i) “publicly available information,” defined as information lawfully made available from federal, state, or government records⁵; (ii) de-identified or aggregated information⁶; (iii) protected health information collected by a covered entity as defined under federal laws including the Health Insurance Portability and Accountability Act; (iv) the sale of information to or from a consumer reporting agency for use in a consumer report consistent with the Fair Credit Reporting Act; (v) personal information about a job applicant or a business’ employees (excluded from most provisions of the CCPA through December 31, 2020); (vi) personal information provided in the context of a business to business communication/transaction (excluded through December 31, 2020); and (vii) personal information collected, processed, sold or disclosed pursuant to the Gramm-Leach-Bliley Act

⁵ [Civil Code Section 1798.140\(o\)\(2\)](#).

⁶ [AB 874](#)

(GLBA) or the Driver’s Privacy Protection Act of 1994, to the extent the CCPA conflicts with those laws.⁷

The exemption for information that is subject to the GLBA is narrow, as the CCPA’s protections apply to a much broader set of personal information than is covered by the GLBA. Entities covered by the GLBA typically collect a good deal of information that is not subject to the GLBA, but that will be subject to the CCPA. Comingled personal information may result in some information, or uses of information, falling within exceptions and other information, or uses of information, not falling within exceptions. For example, personal information that a dealership collects from a consumer to (i) extend credit to that consumer in connection with the purchase of a car for personal, family, or household use, (ii) arrange for that consumer to finance or lease a car for personal, family, or household use, or (iii) provide financial advice or counseling to that consumer would fall under the scope of the GLBA and would therefore not be subject to the CCPA. However, personal information, such as an email address, collected from that consumer that a dealership uses for its own commercial marketing purposes would fall within the scope of the CCPA.

Rights of California Consumers

Under the CCPA, consumers are granted several rights, including:

- **General notice** – Several CCPA sections require businesses to make disclosures to consumers via privacy policies or other notices.
- **Specific information** – The CCPA grants consumers an individualized right to know what personal information a business has collected, sold, or disclosed about them.
- **Data portability** – The specific information rights create what is referred to as a data portability right—the right to obtain a copy of personal information collected about consumers.
- **Deletion**⁸ – The CCPA grants consumers the right to request that a business and its service providers delete their personal information, subject to certain exceptions.
- **Opt-out of the sale of personal information**⁹ – The CCPA grants consumers over 16 years old the right to opt-out of the sale of their personal information. Consumers under 16 are granted a right to opt-in.¹⁰

⁷ [Civil Code Sections 1798.145\(c\),\(d\),\(e\) and \(f\)](#).

⁸ A business shall not be required to comply with a request to delete if the personal information is necessary to fulfill the terms of a written warranty or product recall conducted in accordance with federal law.

⁹ The right to opt-out shall not apply to vehicle information or ownership information retained or shared between a new motor vehicle dealer and the vehicle manufacturer, if the vehicle or ownership information is shared for the purpose of, or in anticipation of, a vehicle repair covered by a vehicle warranty or a recall, provided that the new motor vehicle dealer or manufacturer does not sell, share, or use that information for any other purpose.

¹⁰ Given that information is not collected from consumers under the age of 16 in the regular course of business, this Handbook does not provide detailed guidance surrounding this requirement.

- **Freedom from discrimination** – The CCPA grants a right to equal service, prohibiting discrimination against consumers who exercise their rights.

To comply with the CCPA, businesses must make required disclosures via their privacy policies or other notices, establish processes and procedures to respond to requests to exercise consumer rights (known generally as data subject access requests or DSARs), establish employee training programs, protect personal information that they hold, and review service provider and other third-party agreements for alignment with the CCPA's requirements.

Why is this important?

The CCPA is enforceable both by the California Attorney General and by private litigants. The Attorney General is authorized to pursue civil penalties of up to \$7,500 per violation of the CCPA. The civil penalty for intentional violations is up to \$7,500 and, for other violations, up to \$2,500. The system for civil penalties under the CCPA is the same as that used to enforce the California Online Privacy Protection Act (CalOPPA), a 2003 law which requires website operators to post a privacy policy on their website if the site collects personal information. It is likely that the enforcement of the CCPA will follow the same rules as CalOPPA, meaning damages will be calculated on a per-capita basis—each user whose profile is illegally processed, sold, etc., will represent an independent violation.

Individuals may bring a limited private right of action in connection with “certain unauthorized access and exfiltration, theft, or disclosure of a consumer’s non-encrypted or non-redacted personal information” if the business has failed to implement and maintain reasonable security measures to protect such information.

How long does my dealership have to prepare for the CCPA?

The CCPA is effective January 1, 2020 and companies should strive for compliance by this date. However, the Attorney General cannot bring enforcement actions under the CCPA until July 1, 2020.¹¹

Even though the Attorney General may not bring any enforcement actions under the CCPA before July 1, 2020, the provisions of the CCPA that create a private right of action for data breaches are enforceable beginning January 1, 2020 and it is possible that enforcement actions may be brought based on activity from the beginning of the CCPA effective date. Additionally, a consumer’s request to know the categories and specific pieces of personal information about them that the business has collected or shared requires dealerships to “look back” 12 months

¹¹ Under [Civil Code 1798.185\(c\)](#), the Attorney General cannot bring enforcement actions under the CCPA until July 1, 2020 or six months after the publication of final regulations, whichever is sooner. The Attorney General issued draft regulations in October, 2019. Given that public hearings regarding the proposed regulations were held during the first week of December 2019 and the last day to submit comments was December 6, 2019, final regulations will not be published before the end of 2019. Therefore, the effective date for enforcement will be July 1, 2020.

from the date of the request. In other words, if a request comes in on January 1, 2020, the dealership would need to provide information from January 1, 2019 through January 1, 2020. Thus, dealerships should move quickly in adopting CCPA compliance practices.

The Attorney General's Draft Regulations

In October 2019, the Attorney General issued [CCPA Proposed Regulations](#). Following the comment period which ended on December 6, 2019, the Attorney General will submit the final text of the proposed regulations, the final Statement of Reasons responding to every comment submitted, and an updated informative digest to the Office of Administrative Law (OAL). OAL has 30 working days to review the regulations, and if approved, the rules will go into effect.

The final regulations may differ significantly from the proposed regulations. Nevertheless, it is recommended that dealers implement a CCPA program based on the draft regulations and be prepared to revise the program based on the final regulations when they are eventually published.

II. Determining Whether Your Dealership “Sells” Personal Information

In developing a CCPA compliance program, one of the first steps is to determine whether the dealership “sells” personal information, as that term is defined by the CCPA. If so, unless an exception applies, there are numerous disclosures that must be made and consumers must be afforded specific rights with respect to the sale of their data. Most notably, businesses that sell consumers’ personal information must provide a “reasonably accessible” and “clear and conspicuous” link and/or button on their website’s homepage titled “Do Not Sell My Personal Information.” This link must enable a consumer to opt-out of the sale of their personal information. If a consumer entitled to opt-out, requests to opt-out, the dealership must act within 15 days. The dealership must (i) notify all third parties to whom it has sold information within the past 90 days that the consumer has opted out and to stop selling their information and (ii) it must notify the consumer that this has been completed.¹² (See Section VI of this Handbook for further information regarding opt-outs.)

To avoid this opt-out and numerous other related requirements, you must ensure that you do not sell your consumers’ personal information. Businesses that do not sell personal information are exempt from providing a notice of right to opt-out if the business states in its privacy policy that it does not and will not sell personal information. However, ensuring that your dealership does not “sell” consumer personal information is much more difficult than it sounds because of the broad definition of “sale” under the CCPA and the narrow scope of applicable exemptions and exclusions.

CCPA’s Definition of “Sale”

“Sale” is broadly defined under the CCPA to include 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 to another business or a third party for monetary or other valuable consideration.¹³ The concept of “consideration” under contract law is very broad – it includes “any benefit conferred” to the contracting party, to which that party is not lawfully entitled, absent the agreement.¹⁴

Exceptions and Exclusions

Although the CCPA contains a broad definition of the term “sale,” the CCPA contains various exceptions and exclusions to this term. In addition to the categories of personal information excluded from the CCPA (see Section I), as described below, there are exceptions to the definition of “sale,” and a narrow exception to the opt-out requirement, available only to vehicle dealers and manufacturers. Given the very broad general definition of “sale” under the CCPA, if a dealer intends to avoid installing a “do not sell” button or link on their website

¹² Proposed 11 CCR § 999.315(e),(f)

¹³ [Civil Code § 1798.140\(t\)](#)

¹⁴ [Civil Code § 1605](#)

homepage, the dealer will need to ensure that all sharing of consumer personal information with third parties falls within an applicable exception or exclusion.

Exceptions to the Definition of Sale

The following circumstances, transactions or arrangements are not considered to be a “sale” of personal information under the CCPA:

- When a business uses or shares with a service provider personal information that is necessary to perform a business purpose, if all of the following conditions are met:
 1. The business has provided notice of that information being used or shared in its privacy policy;
 2. The service provider processes the information on behalf of the business pursuant to a written contract that prohibits the service provider 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; and
 3. The service provider does not further collect, sell or use the personal information of the consumer except as necessary to perform the business purpose.¹⁵
- When a consumer directs a business to intentionally disclose personal information to a third party;
- When a business shares with a third party for the purposes of communicating opt-out preferences; and
- In the event of a merger, acquisition, or other corporate sale transaction.¹⁶

Exception to the Right to Opt-out

Thanks to the passage of [AB 1146](#), there is an exception for sharing personal information relating to vehicle warranty and recall repairs. Consumers do not have the right to opt-out when a new vehicle dealer and the vehicle manufacturer share vehicle information (VIN, make, model, year, and odometer reading) or ownership information (names of registered and legal owners), for the purpose of providing a vehicle repair covered by a vehicle warranty or a recall. The exception only applies, however, if the party receiving the information does not sell, share, or use that information for any other purpose.¹⁷

¹⁵ [Civil Code §§ 1798.140\(t\)\(2\)\(C\),\(v\)](#)

¹⁶ [Civil Code § 1798.140\(t\)\(2\)\(A\),\(B\),\(D\)](#)

¹⁷ See [AB 1146](#)

Third-Party Contracts That Allow Access to Personal Information

In order to determine if the dealership is “selling” personal information to third parties, the dealership will need to carefully review its contracts. If third-party companies have access to the dealership’s computer system, and are permitted to use the information for their own benefit, then a “sale” has likely occurred, triggering the requirement to offer the opt-out. It is possible that some businesses may not be able to honor an opt-out request, because a third party has access to all customer contact information, and the businesses’ system is not currently segregated in a way that would only allow access to information of consumers who have not opted out. To avoid this scenario and to potentially avoid the requirement to offer the opt-out, now is the time to renegotiate and amend third-party contracts as necessary. Changes may be required to ensure there is no sharing of personal information that amounts to “selling.” Alternatively, if “selling” personal information will continue, dealerships may need to implement changes so that information of consumers who have opted out will not be shared with third parties. In your negotiations with third parties on this issue, consider reviewing the Sample Data Processing Agreement, or incorporating the language in the short form Service Provider Agreement Regarding Compliance with the CCPA, which are included in Chapter XIV(K),(L) of this Handbook. These sample agreements contain language that could be helpful in your negotiations with third-party vendors on this issue. When reviewing contracts, if it is unclear whether the arrangement amounts to “selling” personal information, dealers are encouraged to seek the advice of knowledgeable counsel.

III. Data Mapping

In developing a CCPA compliance program, one of the early steps that must be tackled is “data mapping.” To provide accurate disclosures and responses to data requests, dealerships will need to determine:

- The categories of personal information collected;
- The sources from which personal information is collected;
- Where personal information is stored;
- Third parties with whom personal information is shared; and
- The purpose for sharing each category of personal information.

It is recommended that dealerships take an inventory of all data collected and shared by every department within the dealership. Data mapping should take into account every method of collection and sharing, including data that is collected/shared by or through the following means:

- Online through webforms or interaction with the dealership’s website;
- Emails;
- Chats;
- Telephone calls; and
- In-person

In going through this exercise, it is important to consider every type of personal information collected or shared. [See the eleven categories of personal information listed in Section I]. Once the dealership finishes mapping its data, it will have the information necessary to complete many of the CCPA disclosure forms and notices described in the following sections of this Handbook.

IV. CCPA Notice at Collection of Personal Information

The CCPA requires businesses to make a visible and accessible disclosure regarding the collection of personal information at or before the point of collection.¹⁸ Under the proposed regulations, this disclosure may be made by reference to a link to the privacy policy when provided online. For offline collection, a link may be provided but additional notice may be needed depending upon the manner in which the dealership primarily interacts with the consumer (e.g., a prominent sign may be needed).

Content of Notice at Collection of Personal Information (Notice)

The Notice must include:

1. A list of the categories of personal information to be collected, written in a manner that provides consumers a meaningful understanding of the information being collected.
2. For each category of personal information collected, the business or commercial purpose(s) for which it will be used.
3. If the business sells personal information, the link titled “Do Not Sell My Personal Information” or “Do Not Sell My Info” required by section 999.315(a), or in the case of offline notices, the web address for the webpage to which it links.
4. A link to the business’s privacy policy, or in the case of offline notices, the web address of the business’s privacy policy.¹⁹

The Attorney General’s regulations further provide that the Notice must be easy to read, understandable to the average consumer (use straightforward language and avoid technical or legal jargon), and must use a format that draws the customer’s attention to the notice.²⁰

(See the Sample Notice at Collection of Personal Information in Section XIV(A))

Translation Requirement

The Notice must be “available in the languages in which the business in its ordinary course provides contracts, disclaimers, sale announcements, and other information to consumers.”²¹ If your dealership advertises in foreign languages, or posts signs in foreign languages, the Notice should be translated into those languages.

¹⁸ [Civil Code Sections 1798.100\(b\)](#)

¹⁹ [Civil Code Sections 1798.100\(b\)](#); proposed 11 CCR § 99305(b)

²⁰ Proposed 11 CCR § 999.305(a)(2)a., b.

²¹ Proposed 11 CCR § 999305(c)

Accessibility Requirement

The Attorney General's regulations require that the Notice must be accessible to consumers with disabilities. At a minimum, a business must provide information on how a consumer with a disability may access the Notice in an alternative format.²² To meet this requirement, the Notice should be posted on the dealership's website in a manner that is accessible to users with disabilities (for example, by using coding to enable blind users with text-to-speech software and/or text-to-Braille hardware to read the Notice). Employees should be trained to direct customers with disabilities to the dealership's website to access the Notice.

How to Provide the Notice

The Attorney General's regulations state that regardless of whether a business collects personal information online or offline, the Notice must be visible or accessible where consumers will see it, before any personal information is collected.²³ Below we address the primary methods by which dealerships collect personal information from consumers:

- **Online:** If a dealership collects personal information from a consumer online, the Notice may be given to the consumer by providing a link to the section of the dealership's privacy policy that contains the "Notice at Collection" information.²⁴ The Regulations state that a business may "conspicuously post a link to the notice on the business's website homepage or the mobile application's download page, or on all webpages where personal information is collected."²⁵
- **Text communications:** Following the initial text message to a consumer, add a link to the dealership's online Notice at Collection.
- **Email signature disclaimer:** Beneath the signature of each email sent by dealership representatives to consumers, add "Your privacy is important to us. See our **Notice at Collection of Personal Information** [INSERT LINK] and **Privacy Policy** [INSERT LINK]."
- **Phone calls:** At some dealerships, certain inbound phone calls have a recording that informs consumers that their calls may be recorded. The dealership should consider adding language directing consumers to view the dealership's online Notice at Collection, such as: "Your privacy is important to us. You may view our Notice at Collection of Personal Information and our Privacy Policy at [URL], or ask a dealership representative for a copy."

²² Proposed 11 CCR § 999.305(a)(2)d.

²³ Proposed 11 CCR § 999.305(a)(2)e.

²⁴ Proposed 11 CCR § 999.305(c)

²⁵ Proposed 11 CCR § 999.305(c)

- **At the showroom:** The Attorney General’s regulations provide that 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 the web address where the notice can be found.”²⁶

We recommend that paper copies of the Notice be held at the dealership if a consumer wishes to take a copy with him/her. At the first instance when personal information is collected (for example before swiping, scanning, or making a photocopy of a consumer’s driver’s license), or completing a customer contact form, a dealership representative should offer to provide a hardcopy of the Notice. Also, dealerships should revise their Privacy Notices to draw consumers’ attention to the dealership’s Notice at Collection and Privacy Policy. The model form Privacy Notice contains space at the bottom of the reverse side, in the section titled, “Other Important Information.” This box may be used (1) to discuss state and/or international privacy law requirements; and/or (2) to provide an acknowledgement of receipt²⁷. We recommend adding the following language to the bottom of the reverse side of the Privacy Notice:

Other important information			
<p>To provide you with additional information regarding our privacy practices and your rights under the California Consumer Privacy Act, a copy of our Notice at Collection of Personal Information has been made available to you. Our Privacy Policy may be accessed at [URL]. By signing below, you acknowledge receipt of this Privacy Notice.</p>			
	_____		_____
Signature	Date	Signature	Date
_____		_____	
Print Name		Print Name	

(See the Sample Privacy Notice in Section XIV(D)).

We also recommend that signs be posted throughout the showroom, in locations where consumers are likely to provide personal information. The sign could provide:

Your privacy is important to us. Before providing personal information, you may view our Notice at Collection of Personal Information at [URL], or ask a dealership representative for a copy.

- **In person in the dealership’s service department:** If your dealership uses electronic repair estimates, add the following language to the estimate: “Your privacy is important to us. See our **Notice at Collection of Personal Information** [INSERT LINK] and **Privacy**

²⁶ Proposed 11 CCR § 999.305(a)(2)e.

²⁷ [79050 Federal Register Vol. 76, No. 245.](#)

Policy [\[INSERT LINK\]](#).” If your dealership uses paper estimates, offer to provide a hardcopy of the Notice at Collection of Personal Information at the first instance when personal information is collected. Also add the following language to the estimate, “For information regarding our privacy practices, a copy of our Notice at Collection of Personal Information has been made available to you. Our Privacy Policy may be accessed at [\[URL\]](#).”

In addition, we recommend that signs similar to the one shown above, be posted in areas where customers of the service department are likely to see them, before they provide personal information.

Notice at Collection for Job Applicants and Employees

Prior to collecting personal information from job applicants or employees, employers must disclose (i) the categories of personal information to be collected and (ii) the purposes for which the categories of personal information shall be used.²⁸ Employers can either alter their existing job applications and employee forms in order to make these disclosures, or create a separate disclosure form. Once collected, personal information regarding job applicants and employees must be safeguarded and protected from data breaches. For the year 2020, personal information provided by job applicants and employees is excluded from the remaining provisions of the CCPA (e.g. data requests).

(See the Sample Notice at Collection of Personal Information for Job Applicants and Employees in Section XIV(B))

²⁸ [Civil Code Section 1798.145](#) [Added by Assembly Bill 25, effective January 1, 2020]

V. Privacy Policy

A dealership's privacy policy ("Policy") would primarily cover online data collection through the website, but should also cover offline collection, such as the collection of personal information from individuals who visit a dealership. It must also address the use, disclosure and sale of personal information and consumers' rights regarding their personal information.

Design and Presentation of Privacy Policy

The Attorney General's Regulations include the following requirements, relevant to California dealers:

- The policy must 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."²⁹
- The policy must be easy to read and understandable to the average consumer. It must use plain and straightforward language, and avoid technical or legal jargon.³⁰
- The format must be readable, including on smaller screens.³¹
- The policy must be available in an additional format (such as a PDF) that can be printed as a separate document.³²

Translation and Accessibility Requirement

Like the Notice at Collection described in the prior section, the privacy policy must be translated into the languages in which the dealership "provides contracts, disclaimers, sale announcements, and other information to consumers."³³ The privacy policy also must be accessible to people with disabilities.³⁴ (See pages 13-14 for further discussion regarding these requirements.)

Elements of a Privacy Policy

The following chart explains the elements of a privacy policy that would live on a dealership's website. While this chart, and the sample privacy policy in Section XIV(C), are designed to provide the basic information disclosures required by the CCPA, it is important to remember that a privacy policy must be **accurate and complete**. Therefore, **your privacy policy must be customized to reflect your business practices**. The sample language below and the

²⁹ Proposed 11 CCR § 999.308(a)(3)

³⁰ Proposed 11 CCR § 999.308(a)(2)a.

³¹ Proposed 11 CCR § 999.308(a)(2)b.

³² Proposed 11 CCR § 999.308(a)(2)e.

³³ Proposed 11 CCR § 999.305(a)(2)c.

³⁴ Proposed 11 CCR § 999.305(a)(2)d.

sample privacy policy in Section XIV(C) may or may not apply to your dealership. Use the sample language as a starting point to craft your own customized privacy policy.

Section Title	Explanation
Title	Title of the policy, e.g., “ Privacy Policy ”
Effective Date.	The “Effective Date” should be displayed at the top of the privacy policy. The privacy policy must be reviewed at least once a year under the CCPA. If an annual review does not lead to any changes, you must add “Last Reviewed” as well so that consumers know the policy was reviewed in accordance with the CCPA’s requirements.
General Overview and Scope.	<p>This section of the policy describes the organization to which the policy applies, as well as the categories of data collection to which the policy applies (i.e., online, offline, or both). It must clearly indicate what entities are covered by the policy, including any subsidiaries or affiliates. Here, the term “DEALERSHIP” should be replaced with the appropriate organization(s)’ name. Sample language is below.</p> <p><i>DEALERSHIP (“DEALERSHIP,” “we,” “us,” or “our”) respects the privacy of the information you have entrusted to us. This Privacy Policy (“Policy”) applies to both the online and offline collection of personal information by DEALERSHIP. By using our website and services (collectively, the “Services”), you acknowledge you have read and understood the terms and conditions of this Policy. If you do not agree to the terms and conditions of this Policy, please do not use the Services.</i></p>
Terms of Use.	A reference should be made to the Terms of Use to notify website visitors that the terms apply to the site and to bind visitors to such terms.
Notice of Arbitration (optional).	<p>If the organization chooses to utilize arbitration for dispute resolution and includes that in the terms, a reference to arbitration must be placed at the top of the policy to provide notice that the provision is further down below. The text should be in all caps to provide more prominent notice regarding the provision. Sample language is below.</p> <p><i>PLEASE NOTE THE ARBITRATION PROVISION SET FORTH BELOW, REQUIRES, EXCEPT WHERE AND TO THE EXTENT PROHIBITED BY LAW, YOU TO ARBITRATE ANY CLAIMS YOU MAY HAVE AGAINST DEALERSHIP ON AN INDIVIDUAL BASIS. ARBITRATION ON AN INDIVIDUAL BASIS MEANS THAT YOU WILL NOT HAVE, AND YOU WAIVE, THE RIGHT FOR</i></p>

	<i>A JUDGE OR JURY TO DECIDE YOUR CLAIMS, AND THAT YOU MAY NOT PROCEED IN A CLASS, CONSOLIDATED, OR REPRESENTATIVE CAPACITY.</i>
Information Collected	<p>The CCPA requires you to provide the categories of personal information collected and for each such category, the source(s) of the information, the purpose(s) for which it is collected and the categories of third parties to whom you have disclosed such information either in a sale or for business purposes.</p> <p>Consider utilizing the categories in the definition of “personal information” from the CCPA text as the starting point for organizing categories for your privacy policy. They include the following: (1) identifiers, (2) personal information categories listed in the California Customer Records statute (Civil Code § 1798.80(e)), (3) protected classifications under California or federal law, (4) commercial information, (5) biometric information, (6) internet or other electronic network activity information, (7) geolocation data, (8) audio, electronic, visual, or similar information, (9) professional or employment-related information, (10) education information, and (11) inferences drawn from other personal information. Additional sample language is below.</p> <p><i>Click here [INSERT LINK] for our Notice at Collection of Personal Information, which lists the categories of personal information we collect from consumers and the purposes for collecting the information.</i></p> <p><i>Below is a chart regarding the personal information we have collected about consumers during the last 12 months:</i></p> <p>[insert chart] similar to sample chart in section XIV(C)]</p>
Cookies and Other Similar Technologies.	<p>Here, the organization must describe the types of cookies and other similar technologies used. Certain third parties, such as Google, require disclosure of the use of their services explicitly in the privacy policy. Sample language is below.</p> <p><i>We, and third parties we allow, use cookies and other similar technologies. Cookies are small text files placed on your device that uniquely identify your device and which a website can transfer to a consumer’s hard drive to keep records of his or her visit to a website. We, or third parties, may use session cookies or persistent cookies. Session cookies only last for the specific duration of your visit and are deleted when you close your browser. Persistent cookies remain on your device’s hard drive until you delete them or they expire. Different</i></p>

	<p><i>cookies are used to perform different functions, which we explain below:</i></p> <ul style="list-style-type: none"> • <i><u>Essential</u>. Some cookies are essential in order to enable you to move around our website and use its features, such as accessing secure areas of our website. Without these cookies, we cannot enable appropriate content based on the type of device you are using.</i> • <i><u>Analytics</u>. We use Google Analytics to measure how you interact with our website and to improve your user experience. To learn more about Google Analytics privacy practices and opt-out mechanisms, please visit the Google Analytics Security and Privacy Principles page at https://support.google.com/analytics/answer/6004245?hl=en. Google also provides a complete privacy policy and instructions on opting-out of Google Analytics at https://tools.google.com/dlpage/qaoptout.</i> • <i><u>Targeted Advertising</u>. We use cookies to compile information on our users' interaction with our website. We use this information to serve ads to you off of our website.</i> <p><i>There are several ways to manage cookies. You can control the use of cookies at the browser level, by instructing your browser to accept cookies, disable cookies, or notify you when receiving a new cookie. Please note that if you reject cookies, you may still use our website, but your ability to use some features or areas of our website may be limited. The Network Advertising Initiative also offers a means to opt-out of a number of advertising cookies. Please visit www.networkadvertising.org to learn more. Note that opting-out does not mean you will no longer receive online advertising. It does mean that the company or companies from which you opted-out will no longer deliver ads tailored to your preferences and usage patterns.</i></p>
<p>Collection and Use of Information From Children.</p>	<p>In the U.S., the Children's Online Privacy Protection Act (COPPA) imposes strict requirements on websites or online services that collect personal information from children under 13. The websites of car dealerships are not directed toward children, and here, the organization would present a notice that it does not collect this information. Sample language is below.</p> <p><i>Our Services are not intended for children. We do not knowingly collect personal information from children, and none of our Services are designed to attract children. In the event that we learn that a person</i></p>

	<i>under the age of 13 has provided personal information to us, we will delete such personal information as soon as possible.</i>
Opt-Out.	<p>Here, the organization would explain the opt-out procedure available with regard to marketing communications. Sample language is below.</p> <p><i>We provide you the opportunity to opt-out of marketing communications by clicking the “unsubscribe” link in email communications or by contacting us using the contact information provided below. We will process your request as soon as possible in accordance with applicable law, but please be aware that in some circumstances you may receive a few more messages until the unsubscribe is processed.</i></p> <p><i>Additionally, we may send you information regarding our Services, such as information about changes to our policies and other notices and disclosures required by law. Generally, users cannot opt out of these communications, but they will be primarily informational in nature, rather than promotional.</i></p>
Third-Party Links.	<p>Here, the organization would present a short notice that it is not responsible for the data collection practices of third parties to whom it may provide links. Sample language is below.</p> <p><i>Our website contains links to other sites. DEALERSHIP is not responsible for the privacy practices or content of such other sites. If you have any questions about how these other sites use your information, you should review their policies and contact them directly.</i></p>
Your California Privacy Rights.	<p>Here, the organization must provide information regarding the rights of California residents, under both CCPA and Shine the Light. Further guidance on how to respond to data subject requests is presented in Section IV of the Handbook. Sample language is below.</p> <p><i>California Civil Code Section 1798.83 permits visitors to the Services who are California residents to request certain information, once a year, regarding our disclosure of personal information to third parties for their direct marketing purposes. To make such a request, please send us an email using the contact information provided below and put “Shine the Light Request” in the subject line of your email.</i></p>

	<p><i>From January 1, 2020, California consumers have the following rights:</i></p> <ul style="list-style-type: none"> <p>Right to know</p> <p><i>You have the right to request information about the categories and specific pieces of personal information we have collected about you, as well as the categories of sources from which such information is collected, the purpose for collecting such information, and the categories of third parties with whom we share such information. Please see above.</i></p> <p><i>You have the right to request information about our sale or disclosure for business purposes of your personal information to third parties in the preceding 12 months. Please see above.</i></p> <p>Right to delete</p> <p><i>You have the right to request the deletion of your personal information. Please note that notwithstanding your request, California law permits us to retain certain categories of personal information for numerous purposes, including to complete a transaction, to perform a contract between you and DEALERSHIP, and to comply with a legal obligation.</i></p> <p>Right to opt-out of sale</p> <p><i>You have the right to opt out of the sale of your personal information to third parties. You can exercise this right through the “Do Not Sell My Personal Information” link in the footers of our websites, when such link becomes available on January 1, 2020.</i></p> <p>[OR]</p> <p><i>We do not and will not sell your personal information to third parties.</i></p> <p><i>We do not sell or knowingly collect the personal information of minors under 16 years of age.</i></p> <p><i>If you would like to exercise one or more of the rights above, please contact us using the contact information provided below. You may designate an authorized agent to make a request on your behalf. Such authorized agent must be registered with the California Secretary of State. We may deny a request from an agent that does not submit proof that they have been authorized by you to act on your behalf.</i></p>
--	---

	<p><i>We may need to confirm your verifiable consumer request before completing your request, and, for example, may ask for you to confirm data points we already have about you. We will only use personal information provided in a verifiable consumer request to verify the requestor's identity or authority to make the request.</i></p> <p><i>We endeavor to respond to a verifiable consumer request within forty-five (45) days of its receipt. If we require more time, we will inform you of the reason and extension period in writing.</i></p>
Public Posting Areas.	<p>If the website contains public posting areas, the organization would include this provision to caution individuals on posting personal information and disclaiming responsibility for information posted in public posting areas. Sample language is below.</p> <p><i>Please note that any information you include in a message you post to any public posting area is available to anyone with Internet access. If you do not want people to know your email address, for example, do not include it in any message you post publicly. PLEASE BE EXTREMELY CAREFUL WHEN DISCLOSING ANY INFORMATION IN PUBLIC POSTING AREAS. DEALERSHIP IS NOT RESPONSIBLE FOR THE USE BY OTHERS OF THE INFORMATION THAT YOU DISCLOSE IN PUBLIC POSTING AREAS.</i></p>
Security.	<p>Explain that no data transmissions over the Internet are 100% secure and describe how you will notify individuals in the event of a data breach. Sample language is below.</p> <p><i>We implement reasonable security measures to ensure the security of your personal information. Please understand, however, that no data transmissions over the Internet can be guaranteed to be 100% secure. Consequently, DEALERSHIP cannot ensure or warrant the security of any information you transmit to us and you understand that any information that you transfer to us is done at your own risk. If we learn of a security systems breach we may attempt to notify you electronically so that you can take appropriate protective steps. By using the Services or providing personal information to us, you agree that we can communicate with you electronically regarding security, privacy and administrative issues relating to your use of the Services. We may post a notice via our website if a security breach occurs. We may also send an email to you at the email address you have provided to us in these circumstances. Depending on where you live, you may have a legal right to receive notice of a security breach in writing.</i></p>

Data Transfers.	<p>If data will be transferred across borders (e.g., to manufacturers in other countries or service providers who are located in other countries), the organization must provide notice of this. Sample language is below.</p> <p><i>DEALERSHIP is based in the U.S. If you choose to provide us with information, please understand that your personal information may be transferred to or within the U.S. and we may transfer your information to our affiliates and subsidiaries or to other third parties, across borders, and from your country or jurisdiction to other countries or jurisdictions around the world. If you are visiting from the EU or other regions with laws governing data collection and use that may differ from U.S. law, please note that you are transferring your personal information to the U.S. and other jurisdictions which may not have the same data protection laws as the EU. We put in place appropriate operational, procedural, and technical measures in order to ensure the protection of your personal information. You acknowledge you understand that by providing your personal information: (i) your personal information will be used for the uses identified above in accordance with this Policy; and (ii) your personal information may be transferred to or within the U.S. and other jurisdictions as indicated above, in accordance with applicable law.</i></p>
Assignment.	<p>This is a standard provision that allows the organization to share information in the event of a corporate transaction. Sample language is below.</p> <p><i>In the event that all or part of our assets are sold or acquired by another party, or in the event of a merger, you grant us the right to assign the personal information collected via the Services.</i></p>
Dispute Resolution and Choice of Law.	<p>If choosing to include an arbitration provision, this is where it would be provided. Sample language is below.</p> <p><i>Except where and to the extent prohibited by law, by using the Services, you and DEALERSHIP agree that, if there is any controversy, claim, action, or dispute arising out of or related to your use of the Services or the breach, enforcement, interpretation, or validity of this Policy or any part of it ("Dispute"), both parties shall first try in good faith to settle such Dispute by providing written notice to the other party describing the facts and circumstances of the Dispute and allowing the receiving party thirty (30) days in which to respond to or settle the Dispute. Notice shall be sent to:</i></p>

- Us, at [insert address] or
- You, at the address we have on file for you.

Both you and DEALERSHIP agree that this dispute resolution procedure is a condition precedent that must be satisfied before initiating any litigation or filing any claim against the other party. IF ANY DISPUTE CANNOT BE RESOLVED BY THE ABOVE DISPUTE RESOLUTION PROCEDURE, YOU AGREE THAT THE SOLE AND EXCLUSIVE JURISDICTION FOR SUCH DISPUTE WILL BE DECIDED BY BINDING ARBITRATION ON AN INDIVIDUAL BASIS. ARBITRATION ON AN INDIVIDUAL BASIS MEANS THAT YOU WILL NOT HAVE, AND YOU WAIVE, THE RIGHT FOR A JUDGE OR JURY TO DECIDE YOUR CLAIMS, AND THAT YOU MAY NOT PROCEED IN A CLASS, CONSOLIDATED, OR REPRESENTATIVE CAPACITY. Other rights that you and we would otherwise have in court will not be available or will be more limited in arbitration, including discovery and appeal rights. All such disputes shall be exclusively submitted to [INSERT NAME OF ARBITRATION SERVICE AND WEBSITE ADDRESS OR EMAIL ADDRESS] for binding arbitration under its rules then in effect, before one arbitrator to be mutually agreed upon by both parties.

The arbitrator, and not any federal, state, or local court or agency, shall have exclusive authority to resolve any dispute arising under or relating to the interpretation, applicability, enforceability, or formation of this Policy, including any claim that all or any part of this Policy is void or voidable.

CHOICE OF LAW

This Policy has been made in and shall be construed in accordance with the laws of the State of California, without giving effect to any conflict of law principles. Any disputes or claims not subject to the arbitration provision discussed above shall be resolved by a court located in the State of California and you agree and submit to the exercise of personal jurisdiction of such courts for the purpose of litigating any such claim or action.

OTHER ARBITRATION AGREEMENTS

In the event of a conflict between this agreement to arbitrate and any other arbitration agreement between you and the Dealership, such as an arbitration agreement contained in a retail installment sale contract, lease agreement, or repair estimate (Other Arbitration

	<i>Agreement), the terms of the Other Arbitration Agreement shall govern and prevail in each instance.</i>
How We Respond to Do Not Track Signals.	<p>California law requires organizations to disclose whether or not they respond to do-not-track signals. Note, the new CCPA Proposed Regulations require that businesses treat user-enabled privacy controls, such as a browser plugin or privacy setting or other mechanism, that signals the consumer’s choice to opt-out of the sale of their personal information as a valid opt-out request. Sample language is below.</p> <p><i>We treat user-enabled privacy controls, such as a browser plugin or privacy setting, that communicates or signals the consumer’s choice to opt-out of the sale of their personal information, as a valid request to opt-out.</i></p>
Modifying the Privacy Policy.	<p>Here, the organization must disclose how it will notify users of changes to the privacy policy. Sample language is below.</p> <p><i>We reserve the right to change this Policy from time to time. When we do, we will also revise the “Effective Date” at the top of this Policy. If we make material changes to the Policy, we will notify you by placing a prominent notice on our website and/or by sending you an email at the email address we have on file for you. We encourage you to periodically review this Policy to keep up to date on how we are handling your personal information.</i></p>
Print this Policy	Click here <i>[insert link]</i> to print a copy of this Privacy Policy
Accessibility	Those with disabilities may access this Privacy Policy in an alternate format by clicking here <i>[insert link]</i>
Languages	In addition to English, this Privacy Policy is available in the following languages: <i>[insert languages and a link for each]</i>
Contact Us. The organization must provide contact information, including, a toll-free number for California residents to exercise their rights.	<p>The organization must provide contact information, including, a toll-free number for California residents to exercise their rights. The contact method must reflect the manner in which the business primarily interacts with the consumer. Sample language is below.</p> <p><i>If you have any questions, comments, or concerns about our privacy practices or this Policy, please contact us at:</i></p> <p><i>[insert contact information, i.e., postal address, email address and toll-free phone number]</i></p>

VI. Guidance on Handling Data Subject Access Requests (DSARs)

The CCPA provides for a number of individual rights: access, deletion, data portability, the right to opt-out of sale, etc. These rights apply to California residents, but some businesses will opt to offer them to all U.S. consumers as it is often difficult to distinguish online where a consumer is located and verifying California residency may have its own challenges. We refer to the individuals who are granted these rights as “data subjects.” Data subjects should be made aware of their rights (in privacy notices and policies) and clear internal processes must be in place to deal with any individual requests properly and within the time frame set out in the CCPA. This Handbook provides information about each type of individual right and when the request can be legitimately refused. It also provides an implementation checklist.

Note, third-party vendors who process customer data should be required by contract to assist your organization in the fulfillment of individual rights requests.

Right to Deletion³⁵

Under the CCPA, data subjects have the right to request that a business delete any “personal information” about the data subject which the business has collected *from* the data subject. This right to deletion, however, is not absolute. For example, if a business maintains consumer information that is de-identified, a business is not obligated to delete this information in response to a consumer request. Also, as discussed above on page 4, “personal information” does not include the following items, which are therefore not subject to the right to deletion:

- Publicly available information, defined as information lawfully made available from federal, state, or government records;
- Protected health information;
- The sale of information to or from a consumer reporting agency for use in a consumer report;
- Personal information about a job applicant or a business’ employees (excluded from most provisions of the CCPA through December 31, 2020);
- Personal information provided in the context of a business to business communication/transaction (excluded through December 31, 2020);
- Personal information collected, processed, sold or disclosed pursuant to the GLBA;
- Personal information collected, processed, sold or disclosed pursuant to the Driver’s Privacy Protection Act of 1994

In addition to these exclusions, there are a number of exceptions to the deletion right. A business or service provider is not required to comply with a data subject’s request to delete if the data subject’s personal information is needed for one or more of the following:

³⁵ [Civil Code Section 1798.105\(a\)](#).

Exception	Example
To complete a transaction. Personal information does not need to be deleted if it is needed to: complete a transaction for which it was collected; provide a good or service requested by the data subject or “reasonably anticipated” within the context of an ongoing business relationship with the data subject; or otherwise perform a contract between a business and a data subject.	A consumer submits a deletion request before the return/refund or warranty time period has elapsed. Information needed to verify the purchase or exercise these rights could be excluded from the data that is deleted.
To fulfill the terms of a written warranty or provide notification of a product recall conducted in accordance with federal law.	The would protect vehicle and product warranty information from deletion until the warranty has expired.
To detect illegal behavior. Personal information does not need to be deleted if it is needed to detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, or prosecute those responsible for that activity.	Dealerships may maintain server logs and other information used to detect and prevent security incidents.
To make repairs. Personal information does not need to be deleted if it is needed to identify and repair errors that impair existing intended functionality.	Dealerships may maintain server logs and other data to identify and fix errors in their software programs.
To exercise free speech. Personal information does not need to be deleted if it is needed to exercise free speech, ensure the right of another consumer to exercise his or her right of free speech, or exercise another right provided for by law.	This protects discourse published online by a company or its users from the requirement to delete such information.
For CalECPA compliance. Personal information does not need to be deleted if it is needed in order for a business to comply with the California Electronic Communications Privacy Act (CalECPA).	This 2015 law requires state law enforcement to get a warrant before they can access certain electronic information. If a dealership has received a government request for the personal information of an individual under the terms of CalECPA, then it does not have to delete that information.
For certain internal uses. Personal information does not need to be deleted if it	For example, this would protect personal information from deletion, such as contact

is needed to enable solely internal uses that are reasonably aligned with the expectations of the data subject based on the data subject's relationship with the business, or to otherwise use the data subject's personal information, internally, in a lawful manner that is compatible with the context in which the data subject provided the information.	information obtained in the course of selling a car, which is reflected in an internal report relating to vehicle sales commissions payable to dealership employees.
Comply with a legal obligation. Personal information does not need to be deleted if it is needed to comply with a legal obligation (e.g., statute or regulation requires that the business maintain documentation relating to the data subject, or to defend against legal claims).	Dealerships may maintain certain personal information that they are required to maintain in accordance with their document retention obligations ³⁶ (e.g., California auto dealers are statutorily required to retain all business records relating to vehicle transactions for 3 years).

Method for Submitting Request to Delete

Businesses must provide two or more designated methods for submitting requests to delete. Acceptable methods include a toll-free phone number, a link or form available online through the business's website, a designated email address, a form submitted in person, and a form submitted through the mail. At least one method must reflect the manner in which the business primarily interacts with the consumer. By way of example, the Attorney General's regulations state that businesses that interact with consumers primarily at a retail location should offer three options: a toll-free number, a form accessible through the business' website and a form that can be submitted in person at the retail location. All requests to delete must be confirmed with the consumer. Therefore, upon receipt of a request, the initial response should also confirm with the consumer that s/he would like to delete the information on file (and the amount of information that the consumer would like deleted, i.e., all or a portion). All such requests will be subject to the exceptions discussed above.

[See the sample form in Section XIV(E) for in-person data requests].

Timing Requirements After Receiving Request for Deletion

Within 10 days of receiving a deletion request, a business must (1) confirm receipt of the request and (2) provide information about how the business will process the request and the

³⁶ Please see Section VII for additional guidance on record retention policies.

business’ verification process (discussed below).³⁷ See the sample Initial Response to Data Request in section XIV(F).

Within 45 days of receiving a deletion request (and regardless of the time required to verify the request), a business must respond to the request. If the business needs more time, the time period can be extended by another 45 days (for a total of 90 days) if the business provides the consumer with notice and an explanation regarding why more time is needed.³⁸

Deletion of Data

Upon receipt of a verifiable data subject request, a business must delete from its records the data subject’s personal information that is not subject to one of the above exceptions or exclusions and direct any service providers to delete such information from their records. For requests to delete, the business must use a two-step process for online requests in order to ensure confirmation. A business can only present the requestor with the choice to delete select portions of their personal information if a global option to delete all personal information is also offered, and is more prominently presented than the other choices. It is recommended that the dealership direct service providers in writing to delete such information from their records and that the dealership obtain written confirmation that the deletion has been completed.

A business may comply with a deletion request by: (i) permanently and completely erasing the personal information on its existing systems with the exception of archived or backup systems³⁹; (ii) de-identifying the personal information; or (iii) aggregating the personal information. If a business stores any personal information on archived or backup systems, it may delay compliance with the request to delete until the archived or backup system is next accessed or used.

If a deletion request is subject to an exception or exclusion, the information should be deleted upon the later of (i) the time when the exception, if applicable, no longer applies or (ii) the expiration of the dealership’s record retention period for the information (see Section VII). Regardless of whether certain information is subject to an exception or exclusion, as a best practice, dealerships should treat all deletion requests as requests to opt-out of marketing communications and, to the extent applicable, also treat such requests as “do not sell” requests. Thus, once a deletion request is received, a dealership should discontinue marketing to the consumer, instruct the dealership’s service providers, in writing, to discontinue marketing to the consumer, and obtain written confirmation that the service providers will do so. Essentially, all use of the consumer’s data should be limited to use in connection with the exception or exclusion relied upon for support in maintaining the personal information instead of deleting it. And in the event a dealership cannot verify a requestor’s identity, the request must be treated as a “do not sell” request.

³⁷ Proposed 11 CCR § 999.313(a)

³⁸ Proposed 11 CCR § 999.313(b)

³⁹ Information on these systems may be deleted the next time the archived or backup system is accessed or used.

Written Response to Request to Delete

In addition to deleting the data, a business must prepare a response to the consumer. In its response, the business must specify the manner in which it has deleted the personal information and disclose that the business will maintain a record of the request pursuant to Civil Code Section 1798.105(d).

If a business cannot verify a requestor's identity, the business must inform the requestor that their request has been denied due to the business' inability to verify their identity and that the request shall instead be treated as a request to opt-out of selling their information.

If a deletion request is subject to an exception or exclusion, the business may deny the request to delete and explain the basis for the denial, including any statutory and regulatory exception that applies. However, the business must delete the consumer's personal information that is not subject to the exception and not use the information that is retained for any purpose other than the purpose for which it is being retained.

If a request is deficient because it was not submitted through one of the designated methods or it is deficient in some other manner unrelated to the verification process, the business must still provide a response. The business can either (1) provide the consumer with specific directions on how to submit the request or remedy any deficiencies with the request or (2) treat the request as if it had been properly submitted through the designated channel.⁴⁰

The dealership's written response to a deletion request will vary, depending on the consumer's interaction with the dealership. See the sample responses in Section XIV(G) for the following categories of consumers:

1. Consumers who have not purchased products or services from the dealership, or applied for credit; but about whom the dealership has collected personal information.
2. Consumers who have applied for credit, but did not buy or lease a vehicle from the dealership (dead deals).
3. Consumers who bought or leased a vehicle; purchased parts, or had their vehicle serviced at the dealership.

Requests to Know

The CCPA grants data subjects the "right to know" what personal information a business has collected, sold, or disclosed about them.⁴¹ The main access-related provision states that "a consumer shall have the right to request that a business that collects a consumer's personal

⁴⁰ Proposed 11 CCR § 999.312(f)

⁴¹ These information access rights are scattered throughout the CCPA, in Sections [1798.100\(a\)](#), [1798.110\(a\)](#), and [1798.115\(a\)](#).

information disclose to that consumer the categories and specific pieces of personal information the business has collected.”⁴² For each category of personal information collected, the business must also disclose the following:

1. **Categories of sources** from which the personal information was collected;
2. **Business or commercial purposes** for collecting the personal information;
3. **Categories of third parties** with whom the business shared or sold the personal information;
4. **Business or commercial purpose for which it sold or disclosed** the personal information.⁴³

Consumers are permitted a maximum of two Right to Know requests in any 12-month period.⁴⁴

Method for Submitting Request to Know

Like requests for deletion, businesses that interact with consumers primarily at a retail location should offer three methods for submitting a Request to Know: a toll-free number, a form accessible through the business’ website and a form that can be submitted in person at the retail location. [See the sample form in Section XIV(E) for in-person data requests].

Timing Requirements After Receiving Right to Know Request

Within 10 days of receiving a right to know request, a business must (1) confirm receipt of the request and (2) provide information about how the business will process the request and the business’ verification process (discussed below).⁴⁵ [See the sample Initial Response to Data Request in Section XIV(F).]

Within 45 days of receiving a Right to Know request (and regardless of the time required to verify the request), a business must respond to the request. This time period can be extended by another 45 days (for a total of 90 days) if the business provides the consumer with notice and an explanation regarding why more time is needed.⁴⁶

Written Response to Request to Know About Categories of Personal Information

After verifying the requester’s identity, a business must provide the consumer with an individualized response, listing the “categories” of personal information collected about the requester. When identifying the categories, refer to the eleven categories enumerated in the personal information definition (see page 4) that most closely describe the personal information at issue in the request.

⁴² [Civil Code § 1789.100\(a\)](#)

⁴³ Proposed 11 CCR § 999.313(c)(10)

⁴⁴ [Civil Code § 1798.100\(d\)](#)

⁴⁵ Proposed 11 CCR § 999.313(a)

⁴⁶ Proposed 11 CCR § 999.313(b)

For each category, the business must disclose the categories of sources of the information, the business purpose for collecting the requester's information, the third-parties with whom the business shared the requester's information, the third-parties with whom the business sold the requester's information and the business purpose for selling or disclosing that information.

As with requests for deletion, if the data request was improperly submitted or is insufficient, the business provide the consumer with specific directions on how to properly submit the request or remedy any deficiencies. Or, the business may choose to treat the request as if it had been properly submitted.⁴⁷

The dealership's written response to a right to know request will vary, depending on the consumer's interaction with the dealership. See the sample responses in Section XIV(H) for the following categories of consumers:

1. Consumers who have not purchased products or services from the dealership, or applied for credit; but about whom the dealership has collected personal information.
2. Consumers who have applied for credit, but did not buy or lease a vehicle from the dealership (dead deals).
3. Consumers who bought or leased a vehicle; purchased parts, or had their vehicle serviced at the dealership.

Response to Request to Know About Specific Pieces of Information

If a business receives a request to disclose the "specific pieces" of information collected about a consumer, the business will need to disclose the actual "personal information" in its records about the consumer, based on the eleven categories of information described above (see page 4). For example, the business might state:

We have collected the following specific pieces of information about you:

Your name: Bobby Buyer

Your phone number: (213) 123-4567

Your email address: BobbyBuyer@gmail.com

Your mailing address: 12345 Main Street, Any Town, CA 99999

When disclosing the specific pieces of information, a business must not disclose 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, or security questions and answers.⁴⁸

⁴⁷ Proposed 11 CCR § 999.312(f)

⁴⁸ Proposed 11 CCR § 999.313(c)(4)

Since one of the categories of personal information is the requester’s signature,⁴⁹ it is likely that each signature the dealership has obtained constitutes a specific piece of personal information that has been collected. Therefore, it appears the dealership will be obligated to produce each document that has been signed, with the information listed above redacted. Dealers would be wise to only have customers sign documents that must be signed, to avoid having to retain and produce documents that otherwise could be disposed of (such as a four-square form).

A response that includes specific pieces of information should be provided in a secure manner. If the dealership’s website does not provide for the secure exchange of information, consider mailing the information to the consumer’s address according to the dealership’s records. If the requested information includes signed documents, it would be appropriate to require the consumer to come to the dealership to obtain the information they have requested, after presenting their unexpired government-issued photo identification. Although the regulations do not address the method of disclosure to be used by retailers that collect sensitive personal information onsite, it seems reasonable that consumers who previously visited the dealership should be required to return to the dealership in order to obtain copies of forms they have signed, along with any other sensitive information that has been collected.

Verification of Requests

Under the CCPA, a “verifiable consumer request” is defined as a request that is made by a consumer, by a consumer on behalf of the consumer’s minor child, or by a natural person or a person registered with the Secretary of State, authorized by the consumer to act on the consumer’s behalf, and that the business can “reasonably verify.”⁵⁰ The Attorney General’s regulations⁵¹ shed some light on how businesses must go about verifying a data request:

1. When possible, match the identifying information provided by the consumer to the personal information already maintained by the business.
2. Avoid collecting sensitive personal information, unless it’s necessary for the purpose of verifying the consumer. Sensitive information includes:

(A) An individual’s first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted:

(i) Social security number.

⁴⁹ [Civil Code § 1798.140\(o\)\(1\)\(B\)](#); [Civil Code § 1798.80\(e\)](#)

⁵⁰ [Civil Code Section 1798.140\(y\)](#)

⁵¹ Proposed 11 CCR §§ 999.318, 999.323(b), 999.325

(ii) Driver’s license number or California identification card number.

(iii) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual’s financial account.

(B) A username or email address in combination with a password or security question and answer that would permit access to an online account.

3. When deciding how stringent the verification process must be, consider the sensitivity of the personal information that the dealership has collected and maintained, the risk of harm caused by complying with an unauthorized request, the likelihood of fraud, the manner in which the business has interacted with the consumer and available technology for verification.
4. If possible, avoid collecting additional information for verification purposes, beyond what is already in your records. If such additional information is requested, delete it as soon as possible after processing the consumer’s request.
5. When verifying deletion requests, verification must range from a “reasonable degree” to a “reasonably high degree” of certainty, depending on the sensitivity of the personal information and risk of harm to the consumer posed by unauthorized deletion. For dealers, most sensitive information would need to be retained if a customer has bought a vehicle from the dealership or had their vehicle serviced there.
6. Requests for access to, or deletion of, household information is allowed if all consumers of the household jointly request access to specific pieces of information. The business must individually verify all members of the household before complying with the request.

To sum it up, in order to verify a consumer, dealers will need to request some identifying information that was previously provided by the consumer. For example, a dealership could compare the requestor’s email address and/or phone number with the customer’s contact information in the dealer’s computer system. A more robust approach would be to authenticate the request by contacting the consumer using the contact information in the dealer’s records. If the information does not match, or the consumer does not respond to the dealership’s authentication communication, the dealership will need to take further steps to verify the consumer before considering their data request. One possibility would be to arrange a video call with the consumer. Ask the consumer to hold up their government ID next to their face, so you can visually confirm that the person is who they claim to be. Or, in the case of a purchase/lease or service customer who requests disclosure of specific pieces of their personal information, the dealership should consider requiring the consumer to come to the dealership and present their unexpired government-issued photo identification. There are also several third-party vendors

offering automated solutions. Be sure to vet them carefully, as they will have access to your customers' data.

There are some exceptions to the verification requirements. For requests to delete, if a business cannot verify the identity of the requestor, the business may deny the request but shall inform the requestor that their identity cannot be verified and must instead treat the request as a request to opt-out of sale.

Authorized Agents

Consumers may use an “authorized agent” to submit data requests on their behalf. An authorized agent must be registered with the California Secretary of State.⁵² A business can require (1) a data request submitted by an agent must be backed by a written authorization by the consumer and (2) the consumer must verify their identity directly with the business.⁵³ The only exception to these two rights is when the authorized agent has a power of attorney to act on the consumer's behalf, in which case the business should consider requiring a certified copy of the power of attorney.

Right to Data Portability

Under the CCPA, the right to access has been merged with the right to data. Where a business responds to an access request “electronically,” it must provide the personal information in a “portable and, to the extent technically feasible, in a readily useable format that allows the consumer to transmit this information to another entity without hindrance.”⁵⁴ There is currently no guidance on what is considered “technically feasible” or “readily useable,” but businesses may look to Article 20 of the EU General Data Protection Regulation for guidance. Article 20 provides for the data to be in a “structured, commonly used and machine-readable format” and also provides for direct transmissions from one controller to another upon request “where technically feasible.” The California Attorney General's final regulations, when issued, may make mention of this language and data portability in general.

Rights Related to the Sale of Personal Information

The right to **opt-out** authorizes data subjects to opt-out of the sale of their personal information by a business. The right to opt-out must be presented to data subjects *before* any selling occurs. A data subject may exercise this right at any time and may also authorize another person to opt-out on their behalf. Businesses that are directed by a data subject or their designee not to sell their personal information may not do so unless the data subject subsequently provides express authorization for such sale. Once a data subject has opted-out, a business must wait at least 12 months before requesting that the data subject authorize its sale. Finally, any

⁵² Proposed 11 CCR § 999.031(c)

⁵³ Proposed 11 CCR § 999.326

⁵⁴ [Civil Code § 1798.100\(d\)](#)

information the data subject provides in connection with their opt-out request must be used solely for the purposes of complying with that request. As noted in Section I, additional requirements apply when dealing with data subjects under the age of 16.

Additionally, the CCPA prohibits businesses from engaging in the resale of personal information (i.e., selling data that was sold to it) without providing consumers explicit notice and an opportunity to exercise the right to opt-out of the resale. This provision may raise challenges for car dealerships in the context of referral websites, in particular, the obligation to provide explicit notice prior to reselling data may be problematic for businesses lacking a first-party relationship with consumers.

Notice of Right to Opt-out

As explained in Section II, businesses that sell consumers' personal information must provide a "reasonably accessible" and "clear and conspicuous" link and/or button on their website's homepage titled "Do Not Sell My Personal Information." Consumers who click on the link should be taken to an "interactive webform"⁵⁵ that will enable them to opt-out. In addition, businesses must offer at least one other opt-out method (such as a toll-free number or email address) and one method that reflects the manner in which the business usually conducts its business (such as an in-person form)⁵⁶. The opt-out notice must be translated into the languages in which the dealership advertises, or provides contracts or other information to consumers.⁵⁷ [See the sample form in Section XIV(E) for in-person data requests].

Responding to Request to Opt-Out

Within 15 days of receiving an opt-out request, a business must notify third parties to whom information has been "sold" within the past 90 days to not further sell the information. In addition, the business must "notify the consumer when this is completed."⁵⁸

Requests to opt-out do not need to be verifiable requests. And businesses must treat user-enabled privacy controls, such as a browser plugin or privacy setting, that communicates or signals the consumer's choice to opt-out of the sale of their personal information, as a valid request to opt-out.

Businesses must maintain records of Data Subject requests and how the business responded for at least 24 months. Include the following in the record: (i) date of request, (ii) nature of request, (iii) manner in which the request was made, (iv) date and nature of the business's response, and (v) if there was a denial, a record of the basis for denial.

⁵⁵ Proposed 11 CCR § 999.315(a)

⁵⁶ Proposed 11 CCR § 999.315(b)

⁵⁷ Proposed 11 CCR § 999.306(a)(2)c.

⁵⁸ Proposed 11 CCR § 999.315(e),(f)

If the business annually buys, receives, or shares the personal information of more than 4 million consumers, the following additional metrics must be tracked regarding the number of requests received, whether the request was complied with in whole or in part, and whether the request was denied. These metrics must be disclosed within the privacy policy (or accessible through a link included in the privacy policy):

- Number of requests to know
- Number of requests to delete
- Number of requests to opt-out
- Median number of days the business took to substantively respond to requests to know, requests to delete, and requests to opt-out.

Data Subject Request Implementation Checklist

- ☐ Set up a privacy inbox, if one has not already been set up, phone number, or utilize an automated solution to deal with requests.
- ☐ Designate the person(s) responsible for receiving requests and ensure they are adequately trained in how to respond.
- ☐ Implement a procedure for verifying the identity of the data subject making the request, if you have reasonable doubts about the identity of the person making the request.
- ☐ Implement a procedure to determine if the request will be granted or denied.
- ☐ If it is determined that the request will be granted, implement a procedure to gather the information that will be provided or prepare the actions that will be taken:
 - Promptly acknowledge the request within 10 days and provide information about how the business will process the request. This information must describe the verification process and when the consumer should expect a response.
 - Resolution and information on action taken in response to a request should be provided **within 45 days** of receipt of the request for requests to know and requests to delete. We note that this period can be *extended* to a maximum of 90 days, but you must promptly respond to the individual and provide a reason for the delay within the initial 45 day period.
 - Respond to requests to opt-out within 15 days from the date of receipt.
 - All communications should be written in a concise, transparent, intelligible, and easily accessible form.
- ☐ Determine which third parties have the relevant personal data and forward the deletion or opt-out requests to them.

- Implement a procedure for logging all individual rights requests, date received, and actions taken. This is important in the event a regulatory authority requests information about your process and responses.

VII. Guidance on Data Retention Policies

A. Elements of a Data Retention Policy

A data (or document, or records) retention policy is a dealership’s established protocol for retaining and disposing of information for operational or regulatory compliance purposes. Such a policy is part of a dealership’s overall data management process and is required by federal and state laws to which a business may be subject. A data retention policy will help a dealership to organize information so it can be searched and accessed at a later date. It will also help a dealership to dispose of information that is no longer needed.

A data retention policy will explain the purpose of the policy, define key terms, describe storage requirements, describe disposal requirements, explain the litigation exception process and how to respond to a discovery request, describe the dealership’s email archival practices, and, finally, provide a document retention schedule. A data retention policy will also factor into the CCPA’s right to deletion. With a clear data retention policy and record retention schedule, certain personal information may fall under the “internal uses” and/or “legal obligations” exceptions to the right to delete.

The following chart explains the information that is required to be contained in a data retention policy as well as sample language for a data retention policy. A sample Data Retention Policy is included in Section XIV(I).

Requirement	Sample Language
Title	DATA RETENTION POLICY
Purpose. This section will explain the purpose of the policy, i.e., compliance with applicable laws.	<p>Purpose</p> <p>The purpose of this Data Retention Policy (“Policy”) is to ensure that the data collected, maintained and used by DEALERSHIP (“DEALERSHIP”), including sensitive personal data, is adequately protected and maintained, and to ensure that data that is no longer needed by DEALERSHIP is discarded at the proper time and in the proper manner. This Policy is designed to ensure compliance with US federal and local laws and regulations, to eliminate accidental or innocent destruction of documents, and to facilitate DEALERSHIP’s operations by promoting efficiency and freeing up valuable storage space. This Policy is also for the purpose of aiding employees of DEALERSHIP in understanding their obligations in retaining information. DEALERSHIP expects all employees to fully comply with this Policy.</p>

<p>Definition of Key Terms. This section will define all key terms in the policy. Typically, “data” or “document”—however, you will be referring to the information—and “retention period” is defined.</p>	<p>Definitions of Key Terms</p> <p>“Data” is defined as any written, recorded or graphic material of any kind existing in any tangible or electronic form that is in the custody, possession or control of DEALERSHIP or any of its directors, officers or employees, which in any way concerns DEALERSHIP’s operations, business activities or legal requirements, including, but not limited to customer personal data. Data may be as obvious as a memorandum, an email, a contract, or something not as obvious, such as a computerized desk calendar, an appointment book, or an expense record.</p> <p>“Retention Period” is defined as the period of time during which Data must be retained. Unless otherwise specified, Retention Periods are measured from the date of Data creation or modification.</p>
<p>Requirements. This section sets forth the policy’s requirements, i.e., what to do and who to contact with any questions.</p>	<p>Requirements</p> <p>All Data will be stored in the physical locations or in the electronic systems that DEALERSHIP has provided and designated for such Data. Data shall be retained in a manner that reasonably protects the Data from damage or destruction, facilitates the location and retrieval of the Data in a minimal amount of time and with minimal expense and effort, and complies with other DEALERSHIP policies and procedures, to the extent applicable. Following the expiration of the Retention Period, Data should be destroyed absent explicit written direction to the contrary from [INSERT TITLE OF PERSON IN CHARGE OF ENFORCING THIS POLICY].</p> <p>Before Data is disposed of or destroyed, DEALERSHIP must verify that the Data (i) has met its Retention Period and (ii) is not the subject of any pending/imminent/threatened litigation or audit (see Section VI below for more information about this exception). Data will be disposed of in a manner that is reasonable considering the content of the Data, but which assures that the information has been destroyed.</p> <ul style="list-style-type: none"> • For printed Data: <ul style="list-style-type: none"> ○ <u>Confidential or sensitive Data</u> should be shredded or incinerated.

	<ul style="list-style-type: none"> ○ All <u>non-confidential Data</u> may be disposed of in the appropriate recycling receptacle. ● For electronic Data: <ul style="list-style-type: none"> ○ All Data should be deleted in a way that is irretrievable and non-restorable.
Email Archival Practices. This section sets forth the business’s practices with regard to email archival. The retention setting will depend on the email platform used by the business.	Email Archival Practices This section is designed to ensure compliance with federal and state laws and regulations, to eliminate accidental or innocent destruction of emails and to facilitate DEALERSHIP’s operations by promoting efficiency and freeing up valuable storage space. This section sets general guidelines, recognizing the impracticality of adhering to rigid rules, and the massive volume of records created by the ever-growing collection of digital devices and services used within DEALERSHIP. DEALERSHIP strives to keep emails as follows: <ul style="list-style-type: none"> ● Retention settings are set to generally “archive” any messages over 6 months of age. These retained messages will be removed from the mail server to reduce the need for storage space. ● The messages will then be archived for up to 7 years, unless a longer or shorter Retention Period is chosen for selected messages. ● Retention settings should apply to all general mail storage folders including inbox and sent messages. ● If an employee uses electronic messages for business, outside a corporate email system account, the employee is expected to make reasonable effort to make records of the messages such that they are within DEALERSHIP’s control.
Litigation Exception Process. The data retention policy must set forth a procedure for what to do in the event of litigation (e.g.,	Litigation Exception Process and How to Respond to Discovery Requests In the event that DEALERSHIP is served with any subpoena or request for Data or any employee becomes aware of a governmental investigation or audit concerning DEALERSHIP or the commencement of any litigation against or concerning DEALERSHIP, such employee shall inform [INSERT TITLE OF PERSON

subpoena, investigation or audit).	<p>IN CHARGE OF ENFORCING THIS POLICY] and any further disposal of Data shall be suspended until such time as [INSERT TITLE OF PERSON IN CHARGE OF ENFORCING THIS POLICY], with the advice of legal counsel, determines otherwise. [INSERT TITLE OF PERSON IN CHARGE OF ENFORCING THIS POLICY] shall take such steps as are necessary to promptly inform all employees of any suspension in the further disposal of Data. This exception supersedes any previously or subsequently established destruction schedule for those Data. If you believe this exception may apply, or have any questions regarding the possible applicability of this exception, or if you believe, for any reason, that Data or category of Data should not be destroyed, please contact [INSERT TITLE OF PERSON IN CHARGE OF ENFORCING THIS POLICY].</p>
<p>Data Retention Schedule. Finally, the data retention policy should list the retention schedules for each type of document the business retains. Certain retention schedules will be dictated by statute or regulation. Others will be business decisions.</p>	<p>Data Retention Schedule</p> <p>It is impossible to designate a Retention Period for each and every type of Data that may exist or come to exist. However, this Policy sets forth Retention Periods for certain common types of Data in the chart below. If certain Data does not fall within a class for which there is a designated Retention Period in this Policy, DEALERSHIP will consult with legal counsel to determine the proper classification of the Data or to establish a Retention Period for the Data in question. To the extent Data is subject to more than one Retention Period, the Data will be retained for the longer of the specified time frames in order to comply with this Policy.</p>

B. Data Retention Schedule

The CNCDA makes available to its members a Record Retention Schedule, prepared by counsel on behalf of CNCDA. The following chart represents a CCPA-specific subset of that schedule and is intended to supplement the dealership's record retention policy. The retention schedule may need to be tailored to the individual dealership.

If a consumer submits a deletion request covering information that (i) is excluded from the definition of "personal information" or (ii) falls under an exception to the deletion right (see page 27), as a best practice, dealerships should treat all deletion requests as requests to opt-out of marketing communications and, to the extent applicable, also treat such requests as "do not sell" requests, even though the dealership is not required to immediately delete portions of the consumer's information from its records. Essentially, all use of the consumer's data should be limited to use in connection with the exception or exclusion relied upon for support in

maintaining the personal information instead of deleting it. As explained in Section VI, the dealership should retain such information until the later of (i) the time when the exception, if applicable, no longer applies or (ii) the expiration of the dealership's record retention period for the information.

DATA RETENTION SCHEDULE		
Description of Record	Retention Period	Commences As Of...
Cash books, cash receipts	6 years	End of year in which books closed.
CCPA requests and responses	2 Years	After date of response
Checks, canceled	10 years	End of year in which check clears; except that copies of checks for important payments should be retained permanently.
Credit applications and all related documents where no sale is made	5 years (recommended) 25 months (mandatory)	After year in which credit application completed.
Credit applications and all related documents where sale is made	10 years (recommended) 7 years (mandatory)	After year of maturity of customer's lease, contract, or extended warranty, whichever comes last.
Credit card, merchant transaction records	6 years (Check merchant agreement and issuer security rules for other requirements)	Date of transaction.
Correspondence, general	4 years	After the later of the year in which correspondence was written, or in which any issues relating to the correspondence are resolved.
Credit memos	6 years	After year issued.
Customer files, deal jackets, vehicle contracts and leases, service contracts	10 years (recommended) 7 years (mandatory if customer applied for credit)	After year of maturity of customer's lease, contract, or extended warranty, whichever comes last.
Emails relating to one of the categories of this retention chart	Period of time for the type of document to which the email refers	See above Data Retention Policy
Miscellaneous emails that do not fit within any of the categories in this chart.	Deleted within 6 months of creation	See above Data Retention Policy
Form 8300 filings	Permanently	N/A

Job applications, resumes, or other employment inquiry submitted in response to an advertisement/notice of job opening, including records pertaining to the failure/refusal to hire any individual	3 Years	After employment decision is made
Motor vehicle ignition keys – data collected prior to origination	2 years	After key is made.
Odometer disclosures (including copy of odometer disclosures on title)	Permanently (recommended) 5 years (mandatory)	After disclosure given or received.
Parts sales slips, parts invoices	6 years	After year in which sold.
Personnel files, including employment applications	7 Years	After end of year in which employment terminated; permanently if any dispute involved
Purchase orders	10 years	After year in which issued; one copy is sufficient.
Rental agreements	7 years	After vehicle returned.
Repair order check sheets	4 years	After year work completed.
Repair orders, office copy and hard copy	6 years	After repairs completed.
Report of sales forms	8 years	Date of transaction.
Sales commission reports	10 years	Date of transaction.
Service contracts, extended warranties	10 years	After year of maturity of customer's lease, contract, or extended warranty, whichever comes last.
Telemarketing compliance materials (internal do-not-call records, national do-not-call downloads, etc.)	9 years	After year in which prepared or obtained.
Vehicle registration correspondence	6 years	After current year.

VIII. Guidance on Data Security

The CCPA heightens the importance of data security at dealerships because it allows consumers to sue businesses for data breaches. If a business maintains consumer data and the data is subject to unauthorized access and disclosure, the CCPA imposes statutory penalties of up to \$750 per consumer per incident, or actual damages, whichever is greater.⁵⁹ However, the CCPA only exposes businesses to liability if the breach is a result of a business's failure to "implement and maintain reasonable security procedures and practices" to protect the data.⁶⁰

In light of these requirements, dealerships should consider reviewing their data security practices with their IT professionals. While the CCPA does not define "reasonable security procedures and practices," California Attorney General has issued guidance on this topic (that predates the CCPA).⁶¹ The Attorney General's guidance references the 20 data security controls published by the Center for Internet Security (CIS) as a baseline for data security.

The following is a brief summary of the 20 CIS data security controls, which you may wish to review with your IT professionals.⁶²

MEASURE	DEALERSHIP CONTROL IMPLEMENTATION
1. INVENTORY AND CONTROL HARDWARE	All connected devices must be continuously documented and authorized. Unauthorized devices are quickly removed.
2. INVENTORY AND CONTROL SOFTWARE	All software must be continuously documented and authorized. Unauthorized software is quickly removed.
3. CONTINUOUS VULNERABILITY MANAGEMENT	Computers are continuously patched. Entire computer system is continuously scanned for vulnerabilities.
4. CONTROLLED USE OF ADMINISTRATIVE PRIVILEGES	Control, log, limit and monitor all administrative access. Use unique system passwords.

⁵⁹ [Civil Code § 1798.150](#).

⁶⁰ [Civil Code Section § 1798.150](#) (a)(1)(A).

⁶¹ California Data Breach Report, California Attorney General (Available at: <https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf>)

⁶² Special thanks to Helion Technologies (<https://heliontechnologies.com/>) for their assistance in the preparation of this chart. Additional information about the 20 data security controls is available the CIS website. (<https://www.cisecurity.org/controls/cis-controls-list/>)

5. SECURE CONFIGURATION FOR HARDWARE AND SOFTWARE ON MOBILE DEVICES, LAPTOPS, WORKSTATIONS AND SERVERS	Deploy computers with vetted, authorized known-secure configurations. Purchase from secure sources. (i.e., not Ebay)
6. MAINTENANCE, MONITORING AND ANALYSIS OF AUDIT LOGS	Enable local logging, cloud based log management and log analytics tools for log analysis.
7. EMAIL AND WEB BROWSER PROTECTIONS	Install current browser versions, control and log internet access. Filter all email external from network.
8. MALWARE DEFENSES	Maintain web-based, logged, continuously updated, regular scanning malware software.
9. LIMITATION AND CONTROL OF NETWORK PORTS, PROTOCOLS, AND SERVICES	Limit installed software, ports and permissions to only those required for operation.
10. DATA RECOVERY CAPABILITIES	Backup and test backups for all data systems. Ensure they are encrypted and stored offsite.
11. SECURE CONFIGURATION FOR NETWORK DEVICES, SUCH AS FIREWALLS, ROUTERS, AND SWITCHES	Maintain standard documented configuration rules. Install latest versions of secure software.
12. BOUNDARY DEFENSE	Document all network boundaries, maintain Intrusion Detection/Prevention and NetFlow.
13. DATA PROTECTION	Manage encryption, storage, access and removal of organizations data at all times.
14. CONTROLLED ACCESS BASED ON THE NEED TO KNOW	Restrict and monitor all network and file access based on required access.
15. WIRELESS ACCESS CONTROL	Maintain secure, inventoried, updated, multi-factor access control WiFi network.
16. ACCOUNT MONITORING AND CONTROL	Continuous inventory of accounts with process to grant and revoke access. Two factor authentication, logging and monitoring.
17. SECURITY AWARENESS AND TRAINING PROGRAM	Workforce gap analysis. Continuous content updates, workforce testing and remedial workforce training.

18. APPLICATION SOFTWARE SECURITY	Use updated and patched third-party software.
19. INCIDENT RESPONSE AND MANAGEMENT	Document and test procedures and designate incident managers. Publish reporting and response directives to organization.
20. PENETRATION TESTS AND RED TEAM EXERCISES⁶³	Establish a penetration testing program. Perform regular internal and external penetration tests and Red Team exercises.

See the CIS Critical Security Controls for Effective Cyber Defense Checklist in Section XIV(J), to assist in determining whether the dealership and its vendors have reasonable security measures in place.

⁶³ A Red Team imitates real-world attacks. By assuming the role of an attacker, they expose vulnerabilities that pose a threat to the organization's cybersecurity.

IX. Template CCPA Compliance Checklist for Vendors

Under the CCPA, a dealership collecting personal information must also ensure that vendors processing data on the dealership's behalf are assisting with legal compliance. This due diligence process should be conducted for current vendors who have not gone through the due diligence process and for any new vendors as part of the onboarding process. Vendors include, without limitation, third-party marketing agencies. We recommend interviewing service providers regarding their compliance with the CCPA. The following checklist will help dealerships assess whether a vendor is compliant, or planning to be compliant with the CCPA:

- ☐ Has the vendor conducted an internal review to confirm what personal information is being collected and/or processed by said vendor?
- ☐ Has the vendor reviewed internal policies and procedures as to the scope and purpose of such collection and/or processing of personal information?
- ☐ Has the vendor reviewed and updated online privacy policies to comply with the CCPA's disclosure requirements?
- ☐ Does the vendor have policies and procedures to ensure it can respond to consumer requests for access to, deletion from, or information related to the sale or disclosure of their personal information? Does it have a policy to assist your business in fulfilling these requests? Who will be paying for any costs involved?
- ☐ Does the vendor have training materials to train all the people within its organization, especially personnel who will be responsible for handling consumer personal information inquiries?
- ☐ Does the vendor have reasonable security measures in place? For a sample list of reasonable security measures, please see the CIS Critical Security Controls in Section VIII above and in Section XIV(J) below.

X. Data Processing Addendums for Vendor Agreements

The following guidance is intended to assist businesses in drafting and/or negotiating agreements with vendors when personal information is involved in a service provided by a vendor. Certain vendors may ask a business to review and agree to the vendor’s data processing agreements. In other cases, the template agreement with a vendor may not adequately address privacy and security. We suggest ensuring language covering the following items is included in any agreement with vendors where personal information is involved:

1. *Defining Personal Data*

The first step in any contract involving personal information is understanding the type of personal information flowing between the parties. Some contracts may clearly define it; others may not. While it is not required that the contract identify what constitutes personal information, some may. California currently has the broadest definition: “personal information” is any information that the vendor has received or collected for processing pursuant to the agreement that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, to a particular consumer or household.

2. *Ownership*

The contract should call out which party owns the personal information at issue in the agreement. Some things to consider when determining who owns the personal information:

- Which entity is making the decisions with respect to what personal information is collected, how it is used, and generally how to control it;
- Which entity is named to the consumer as being responsible for the personal information;
- Which entity is in physical control of the personal information;
- Which entity is making the decisions with respect to what IT systems to use to collect the personal information, how to store it, and what means to use to delete or dispose of it; and
- Whether one entity is being directed by the other with respect to the personal information, including how to use or process the personal information.

Example: *Each party hereby acknowledges and agrees that Dealership owns all right, title and interest in and to the personal information which is processed by Vendor on behalf of Dealership pursuant to this Agreement.*

3. *Applicable Law*

Rather than call out specific privacy laws that may apply, we recommend including language both parties agree on to comply with all applicable data protection law. We suggest avoiding specific language that implies you are subject to or abiding by laws in other countries.

4. *Limitation on Use*

Typically, the contract should limit the vendor's use of personal information. Under the CCPA, contracts with service providers (distinct from other third parties) must specifically prohibit use of personal information for purposes outside of your business relationship. A service provider also shall not use personal information received for the purpose of providing services to another person or entity. Depending on the services provided by the vendor, it may not make sense to limit the use of the personal information. A service provider is allowed to combine personal information received to the extent necessary to detect data security incidents or protect against fraudulent or illegal activity.

Example 1: Vendor must only process personal information in accordance with Dealership's documented instructions, which may be specific instructions or standing instructions of general application in relation to the performance of Vendor's obligations under this Agreement, unless otherwise required by law.

Example 2: Vendor shall not (i) sell the personal information or share the personal information with any third parties without Dealership permission; (ii) retain, use or disclose the personal information for any purpose other than the purposes specified in this Agreement, including retaining, using or disclosing the personal information for a commercial purpose other than to provide Vendor's services to Dealership; or (iii) retain, use or disclose the personal information outside of Vendor's business relationship with Dealership.

Alternatively, you could consider using language from both Examples 1 and 2, if applicable.

5. *Subprocessing*

A subprocessor is a third party that the vendor uses to help it process or manage the personal information. The contract should ensure that the vendor will give notice of changes to subprocessors, require subprocessors to enter into agreements with at least the same level of protection as the contract between the vendor and Dealership, and will remain liable for acts and omissions of any subprocessors.

Example: Dealership grants Vendor a general authorization to use subprocessors to provide the services outlined in this Agreement. Vendor will provide Dealership a list of all current subprocessors. In the event Vendor makes changes to its list of subprocessors, it will notify Dealership immediately and Dealership will have the opportunity to reasonably object to the appointment of any new subprocessors.

Vendor must subject subprocessor to a written agreement which imposes on the subprocessor the same obligations that are imposed on Vendor under this Agreement. Vendor will remain liable to Dealership for any acts or omissions of any subprocessor to the same extent

Vendor would be liable if performing the services of each subprocessor directly under the terms of this Agreement.

6. Cross Border Transfers

Where a vendor is located outside of the US, or has servers outside of the US, we may recommend including language addressing the cross border transfer of personal information depending on the relevant country's data privacy laws. You should consult counsel if the vendor does transfer personal information across borders, as it may lead to additional legal hurdles.

7. Reasonable Security

The contract should address the security of the personal information.

Example: *Vendor must, at a minimum, implement and maintain appropriate technical and organizational measures to ensure the security and protection of personal information, taking into account the nature and sensitivity of the personal information to be protected, the risk presented by processing, the state of the art, and the costs of implementation, in compliance with applicable data privacy legislation.*

8. Security Incidents

The contract should define “data security breach” and place certain obligations on the vendor with respect to handling a data security breach.

Example: *“Data Security Breach” means any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, access to, acquisition of or use of any personal information.*

Vendor must immediately notify Dealership if it knows, discovers or reasonably believes there has been a Data Security Breach. In the event of a Data Security Breach, Vendor must: (i) immediately investigate, correct, mitigate, remediate and otherwise handle the Data Security Breach, including without limitation, by identifying personal information affected by the Data Security Breach and taking sufficient steps to prevent the continuation and recurrence of the Data Security Breach; and (ii) provide information and assistance needed to enable Dealership to evaluate the Data Security Breach and, as applicable, to comply with any obligations to provide timely notice to affected individuals or information about the Data Security Breach to relevant regulators.

9. Liability for Security Incidents

The contract should impose liability on the vendor for data security breaches that are caused by the vendor or vendor's subprocessor.

Example: *Vendor will reimburse Dealership for the reasonable expenses that Dealership may incur as a result of a Data Security Breach caused by Vendor’s acts or omissions or those of any of Vendor’s subprocessors, including but not limited to, the expenses incurred in investigating the Data Security Breach and notifying affected individuals and providing these individuals with the support necessary under the circumstances, such as credit monitoring.*

10. Limitation of Liability

In addition to specifically calling out liability for security incidents, the contract should have a general liability provision. Given the high costs that can be associated with data breaches, many vendors will seek a liability cap. If the vendor insists on a liability cap, we recommend a liability cap of at least \$1 million. This amount, however, may be subject to change given the type of personal information at issue.

Example: *Notwithstanding anything to the contrary in the Agreement, Vendor’s total aggregate liability, including any liability for subprocessors, under or in connection with the Agreement, shall not exceed \$1,000,000.*

11. Indemnity

The vendor should indemnify and hold harmless Dealership.

Example: *Vendor will indemnify and hold harmless Dealership and its officers, directors and employees from and against all third-party claims and legal actions brought against Dealership arising out of Vendor’s breach or alleged breach of the Agreement, or in the event of any injury to any person, damage to or loss of property, or any other claim arising out of or resulting from any act or omission of Vendor, its employees, agents or subprocessors in connection with or arising out of the performance of the Agreement, including without limit, any losses, liabilities, damages, judgments, fines, penalties, costs or expenses including court costs and reasonable legal and investigation costs awarded against or incurred by Dealership. Dealership shall have the right, at its cost, to participate in the defense of any claims concerning matters that relate to Dealership. Vendor may not enter into any settlement without Dealership’s express written consent (which shall not be unreasonably withheld), unless such settlement (i) releases Dealership in full for all claims, (ii) does not impose any obligation on Dealership, other than amounts to be paid directly by Vendor (and not Dealership), and (iii) includes no admission of any kind by or on behalf of Dealership.*

12. Consumer Requests Under the California Consumer Privacy Act (CCPA)

When the dealership provides notice of a deletion request, the vendor should be required to confirm in writing that the consumer’s information has been deleted. If one of the dealership’s customer’s makes a deletion request or other data request directly to the vendor, the vendor should agree to immediately notify the dealership and then act in accordance with the dealership’s instructions.

Example: *If Dealership provides written notification to Vendor of a consumer's request to delete his or her Personal Data, within ten (10) business days of the date the request is sent, Vendor shall delete all such information from Vendor's records and provide written confirmation to Dealership that the information has been deleted. CCPA deletion requests shall be sent by email to Vendor at the following email address [INSERT EMAIL ADDRESS] or by U.S. mail to Vendor's address at [INSERT POSTAL ADDRESS]. If a consumer whose information is subject to this Agreement makes a deletion request or other data subject request directly to Vendor, Vendor shall notify dealership at the following email address [INSERT EMAIL ADDRESS] or by U.S. mail to Dealership's address at [INSERT POSTAL ADDRESS]. Dealership will provide Vendor with instructions for handling the request in compliance with the CCPA and Vendor agrees to act in accordance with Dealership's instructions.*

(See the Sample Data Processing Agreement in Section XIV(K)) and the short form Service Provider Agreement Regarding Compliance With CCPA in Section XIV(L)

XI. Incident Response Manuals

An incident response manual—often called an incident and breach response plan—explains the procedure that must be followed in the event of a data security incident, involving either paper or electronic files. Data security incidents are on the rise and it is almost an inevitability that a business will suffer some type of incident. Some incidents lead to massive network or data breaches that can impact a business for days or even months. When a significant disruption occurs, your organization needs a thorough, detailed plan to help IT stop, contain, and control the incident quickly.

In addition to helping remediate data loss and get systems back up and running promptly, prompt attention to incidents is also important to help protect a business' reputation and limit the loss of customer trust. Studies have shown that customers are likely to take their business elsewhere if they are directly affected by a data breach. If a breach is not properly handled quickly and responsibly, a business risks losing some or all of its customer base.

Finally, a thorough incident response manual helps safeguard a business from potential loss of revenue. Not only is direct revenue at stake in a breach due to the requirement to take systems offline or the corruption of revenue-generating databases by a potential hacker, but the dealership may also face significant costs for legal expenses, remediation, forensic investigations, and regulatory and compliance fines. The faster a business can detect and respond to a security incident, the less likely it will have a significant impact on revenue.

For these reasons, it is important to have a detailed incident response manual ready to go and to ensure that all appropriate employees are trained on what to do in the event of an incident.

(See the Sample Incident Response Manual in Section XIV(M))

XII. Guidance on Cyber Liability Insurance

1. Overview

Cyber liability insurance is liability insurance providing coverage for a series of first- and third-party claims that generally emerge from a business's digital operations, data storage, and data operations. First-party coverage provides insurance for incidents where business operations are impacted or negatively affected, including through ransomware, data breaches, or security incidents in which the company's data is lost, stolen, or made unusable. Third-party claims involve claims made against the insured business by some third party, whether that is an individual, a competing business, or a governmental actor. Different suites of cyber liability coverage provide coverage for different combinations of harms, and may interact differently with various other policies purchased by the insured business, and relevant laws which will apply to the insured business.

Generally speaking, cyber liability coverage is best deployed in concert with other policies providing industry and operation specific coverage tailored for the business. Cyber liability insurance will be a key cog, protecting the insured business's digital operations, its data storage and collection efforts, and provide coverage in the event of a catastrophic failure to the business's computer systems. Much of this coverage does not overlap with, or is explicitly excluded from coverage under other policies, thereby necessitating cyber liability coverage for businesses that collect data, offer technology services to clients, and maintain large computer-based operations.

Lastly, and unlike many other types of coverage, cyber liability coverage includes coverage for data breach events, including both the costs for forensic investigations and immediate remediation and restoration of affected systems, but also for costs related to government and regulator investigations, enforcement actions, and litigation. These coverages can be instrumental in recovering from a cyber-attack, malware attack, or an incidental data breach incident, and can help a business get back on its feet or return to operational capacity sooner than it would without such coverages.

2. Common Coverages Contained in Cyber Liability Policies

a. Information Security and Privacy

Information security and privacy coverage protects businesses in the event that they suffer a data breach or incident and litigation is commenced against them based on it. This coverage provides for defense costs and liability funds to be made available in the event third-parties bring claims resulting from loss or theft of personal information from an insured company's system, and the failure to use reasonable security measures to prevent it or the failure to timely disclose such breach. With respect to data breaches, this can often be the largest cost in the event of a privacy class action suit brought by various individuals whose data may have

been leaked or exfiltrated, and defense fees can be massive depending on the number of affected individuals.

b. Privacy Notification and Crisis Management Costs

This coverage specifically provides funds for the notification of victims of a data breach. When a business hosting or storing data suffers a data breach, the required notification costs can add up quickly depending on the number of individuals whose data was accessed or acquired. This coverage makes funds available to pay legal counsel to prepare and issue those notifications as required, and pay vendors to spread the notification in compliance with relevant state law. Similarly, in events with the potential to negatively impact the insured business's overall business, funds are made available for crisis management, commonly through retention of a public relations firm to guide the insured business through the notification process to minimize the overall impact of the incident.

c. Regulatory Defense and Penalties Coverage

This coverage provides for defense costs for legal counsel to defend the insured business against investigations and regulatory actions filed by governmental actors to enforce the terms of privacy statutes against allegedly infringing businesses. These funds may also provide some or all of the penalties sought by those regulatory authorities, whether through court order or settlement, to the extent such penalties are insurable under the law. Different states allow different amounts of coverage for such penalties, and counsel familiar with the enforcing state's laws will be better positioned to advise on the recoverability of such penalties.

d. Business Continuity and Lost Profits Coverage

This first-party coverage is called upon when some event causes an outage or downtime in the insured business's computer system, preventing the normal operation of the business. This coverage provides for the recovery and remediation of the problem using either internal or external business resources and vendors, and provides a means for the affected entity to calculate and seek the profits it would have earned during the period the business could not operate using historical figures.

e. Technology Errors and Omissions Coverage

When a business performs technology services for its clients, whether that is in the form of data processing, data hosting or storage, or access to an online tool, portal, or service, then coverage may be available for claims of negligence in the providing of those services. Such coverage takes the form of defense payments and liability funds for those non-intentional failures by the insured entity of the proper performance of those services, or of the failure to make those services active when they were otherwise obligated to provide them. This coverage is very similar to professional errors & omissions coverage (such as for attorneys, accountants, or architects), and is often drafted as a direct analogue to such coverage.

f. Intellectual Property Coverage

Certain cyber liability policies provide express coverage and defense and liability funds for so-called “soft” intellectual property disputes, including claims of trademark and copyright infringement and other affiliated claims. These may include trademark or trade dress infringement and dilution, false designation of origin, false association, false advertising, and other similar causes of action against the insured business. This coverage is less common overall in newer cyber liability policies, although it may still be available depending on the form used by the carrier. This coverage may also be added on as an endorsement for an additional fee from the insured business at the time the policy is issued.

3. Potential Coverages Relevant to the CCPA

Coverage under cyber liability policies should be explicitly sought for litigation brought under the CCPA by both individual actors and governmental regulators and authorities and those authorities’ related investigations. While there is unlikely to be coverage for typical “compliance” activities and systemic reviews of data policies, cyber liability policies should be investigated to determine whether the terms may be read to extend coverage for CCPA-related litigation and investigations, as those will likely be the largest single driver of new costs upon enforcement of the CCPA once the CCPA enforcement period begins.

XIII. Intersection of the CCPA and California Franchise Law

Once the CCPA takes effect, California’s legislature and courts will need to weigh in on several important questions. For example, are manufacturers or DMS providers obligated to indemnify for their failure to comply with a dealer’s request on behalf of its customer’s lawful data deletion demand? Existing law points to the answer being “yes.” For example, California [Vehicle Code Section 11713.13\(f\)\(1\)\(C\)](#) mandates that factories indemnify dealers for “[i]mproper use or disclosure by a manufacturer or distributor of nonpublic personal information obtained from a franchisee concerning any consumer, customer, or employee of the franchisee.” Vehicle Code Sections [11713.3\(v\)](#) and [11713.25](#) protect consumers and car dealers from unauthorized access to data by manufacturers and computer vendors (i.e. DMS providers). These laws make it unlawful for an automobile manufacturer, distributor or computer vendor to “access, modify, or extract information from a confidential dealer computer record or personally identifiable consumer data from a dealer without first obtaining express written consent from the dealer and without maintaining administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of the information.” [Vehicle Code Section 11713.25\(a\)\(3\)](#) also mandates that computer vendors shall not “[u]se electronic, contractual, or other means to prevent or interfere with the lawful efforts of a dealer to comply with federal and state data security and privacy laws and to maintain the security, integrity, and confidentiality of confidential dealer computer records, including, but not limited to, the ability of a dealer to monitor specific data accessed from or written to the dealer computer system.”

Data deletion requests and data breach risks increase the need for the strong indemnification provisions set forth in this Handbook. Dealers will need to negotiate with and seek cooperation from their manufacturers, DMS providers and other vendors. Dealerships should also consult with counsel on a case-by-case basis to determine whether pre-existing laws and agreements affect obligations under the CCPA.

XIV. Sample Documents

The following documents are sample documents that can be used by dealerships as a starting point. However, we caution against using the sample documents below without consulting with counsel and confirming the documents are tailored to your practices and needs.

Also, please note these sample documents are based on the Attorney General’s **proposed** regulations. The final regulations that will be published in 2020 may vary significantly from the proposed regulations. If so, it will be necessary to revise many of the following sample forms.

A. Sample Notice at Collection of Personal Information

Notice at Collection of Personal Information

[Name of Dealership] ("Dealership," "we," "us" or "our") respects the privacy of the information our customers entrust to us. This Notice at Collection applies to both the online and offline collection of information. [\[Insert either of the following statements:\]](#) We do not and will not sell personal information / We sell personal information unless you instruct us not to do so by clicking [Do Not Sell My Personal Information](#) [\[add link\]](#) or by visiting [\[insert URL for do not sell / button\]](#). For more information regarding our privacy practices and consumer rights under the California Consumer Privacy Act, view our Privacy Policy at [\[insert URL for Privacy Policy\]](#).

Categories of personal information we collect from you	The business or commercial purpose(s) for which it will be used:
Identifiers , such as: Name, postal address, email address, IP address, identification numbers (e.g., social security number, driver's license number, state identification number, military identification number or passport number)	To respond to your requests and inquiries; communicate with you regarding our products or services; enter into transactions with you; process your transactions; send you marketing communications; complete government forms; confirm your identity and that you are at least 18 years old; and/or confirm you are licensed to drive our vehicles or take delivery of a vehicle you have purchased or leased from us
Other personal information described in Civil Code Section 1798.80(e) , such as: Phone number; insurance information; bank account number, credit card number, debit card number, or other financial information; and/or your signature	To respond to your requests and inquiries; communicate with you regarding our products or services; enter into transactions with you; process your transactions; send you marketing communications; confirm your insurance coverage; confirm your identity; obtain authorization to collect payment from you; collect payment from you; confirm acknowledgement of receipt of documents we provide to you; and/or to complete government forms
Physical description and characteristics of protected classifications under California or federal law , such as: A photocopy/scan of government issued identification reveals personal information. For example: <ul style="list-style-type: none"> • Driver's license/state identification card - includes your image, date of birth, physical description and gender • Permanent resident card - includes your image, date and place of birth; • Social security card - includes your social security number • Passport - includes your image, date and place of birth and your nationality • Military ID - includes your image and rank Completion of a Translated Contract Acknowledgement or signing of translated documents reveals your primary language	To confirm your identity; confirm you are licensed to drive our vehicles or take delivery of a vehicle you have purchased or leased from us; confirm eligibility for a manufacturer/lender rebate and to apply for and process any such rebate; determine coverage under the Military Lending Act; provide you with copies of certain documents written in the language in which your transaction was primarily negotiated, as required by law; and/or to complete government forms
Commercial information from selling/providing products or services to you , such as: Information, including vehicle information and ownership information, regarding a transaction in which we sell or lease a vehicle to you and/or buy a vehicle from you, or provide parts, service repairs to, or maintenance or inspection of your vehicle	To process your transactions; appraise your current vehicle; send you informational and marketing communications; retain records of transactions as required by law; fulfill the terms of a written warranty or product recall; to process warranty, insurance or service contract claims; and/or to share information with state agencies as required by law
Biometric information : If you will be financing or leasing a vehicle from us, we collect a copy of your thumbprint if you complete a "Thumbprint form"	To confirm your identity
Internet or other electronic network activity information , such as: IP address, browsing history, and search history	To communicate with you regarding our products and services; improve user experiences by making our website easier to use and navigate, and more personalized based on the profile we create about you
Geolocation information , such as: Location of IP address or location of vehicle (GPS) - with your consent	To respond to your requests and inquiries; enter into transactions with you; process your transactions; and send you marketing communications.
Audio information , such as: Voicemail messages and/or recorded phone calls (with your consent)	To communicate with you; some phone calls are recorded (with your consent) for training our staff and for quality assurance purposes
Professional or employment related information , such as: Information regarding current occupation	To determine eligibility for a manufacturer/lender rebate and process applicable rebate; and/or to complete government forms, as required
Education information , such as: Information regarding whether you are or will soon be a college graduate	To determine eligibility for a manufacturer/lender rebate and process applicable rebate, if applicable
Inferences drawn from information collected to create a profile , such as: Information regarding your vehicle preferences and needs	To communicate with you regarding our products and services and to market to you
Credit information , including employment information, if you apply to finance or lease a vehicle, or make full payment by check.	See our Privacy Notice [add link]

(Rev. 1/2020)

B. Sample Notice at Collection of Personal Information – Job Applicants and Employees**Notice at Collection of Personal Information – Job Applicants and Employees**

[Name of Dealership] (“Dealership,” “we,” “us” or “our”) respects the privacy of the information job applicants and our employees entrust to us. This Notice at Collection applies to both the online and offline collection of information. We do not and will not sell your personal information. For more information regarding our privacy practices, view our Privacy Policy at [insert URL for Privacy Policy].

Categories of personal information we collect from you	The business or commercial purpose(s) for which it will be used:
Identifiers , such as: Name, postal address, email address, IP address, identification numbers (e.g., social security number, driver’s license number, state identification number, military identification number or passport number)	To communicate with you; consider your suitability for employment; run background checks (with your consent); check your driver’s license status and driving record (if you will be driving our vehicles); verify your identity; populate and administer employment-related documents, payroll, withholding, and employee benefits (if hired); confirm your eligibility to work in the United States; and/or to complete government forms
Other personal information usually collected for customer records, described in Civil Code Section 1798.80(e) , such as: Phone number; bank account number; insurance policy number and/or your signature	To communicate with you; run background checks (with your consent); verify your identity; enable payroll or reimbursement direct deposits (if hired); confirm acknowledgement of receipt of documents we provide to you; obtain any consents needed for contractual purposes; and/or to complete government forms
Physical description and characteristics of protected classifications under California or federal law , such as: A photocopy/scan of government issued identification reveals personal information. For example: <ul style="list-style-type: none"> • Driver’s license/state identification card - includes your image, date of birth, physical description and gender • Permanent resident card - includes your image, date and place of birth; • Social security card - includes your social security number • Passport - includes your image, date and place of birth and your nationality 	To confirm your identity; check your driver’s license status and driving record (if you will be driving our vehicles); confirm your eligibility to work in the United States; and/or to complete government forms
Sensory data , such as audio information: Voicemail messages and/or recorded phone calls (with your consent)	To communicate with you; some phone calls are recorded (with your consent) for training our staff and for quality assurance purposes
Professional or employment related information , such as: Information regarding employment history and employment references	To consider your suitability for an employment position and to check your references
Education information , such as Information regarding your education history and/or degrees	To consider your suitability for an employment position
Health Information , such as Alcohol and drug screen results, information relating to employee leaves and requests for disability accommodations	To consider your suitability for an employment position; and evaluate and/or process leaves of absence or disability accommodations

(Rev. 1/2020)

C. Sample Privacy Policy

Privacy Policy

Effective Date: **[INSERT]**

DEALERSHIP (“DEALERSHIP,” “we,” “us” or “our”) respects the privacy of the information you have entrusted to us. This Privacy Policy (“Policy”) applies to both the online and offline collection of personal information by DEALERSHIP. By using our website and services (collectively, the “Services”), you acknowledge you have read and understand the terms and conditions of this Policy. If you do not agree to the terms and conditions of this Policy, please do not use our Services.

Your use of our Services is also governed by our Terms of Use **[INSERT LINK]**.

PLEASE NOTE THE ARBITRATION PROVISION SET FORTH BELOW, WHICH MAY, EXCEPT WHERE AND TO THE EXTENT PROHIBITED BY LAW, REQUIRE YOU TO ARBITRATE ANY CLAIMS YOU MAY HAVE AGAINST DEALERSHIP ON AN INDIVIDUAL BASIS. ARBITRATION ON AN INDIVIDUAL BASIS MEANS THAT YOU WILL NOT HAVE, AND YOU WAIVE, THE RIGHT FOR A JUDGE OR JURY TO DECIDE YOUR CLAIMS, AND THAT YOU MAY NOT PROCEED IN A CLASS, CONSOLIDATED, OR REPRESENTATIVE CAPACITY.

INFORMATION COLLECTED

Click **here** **[INSERT LINK]** for our Notice at Collection of Personal Information, which lists the categories of personal information we collect from consumers and the purposes for collecting the information.

Below is a chart regarding the personal information we have collected about consumers during the last 12 months:

Category of personal data	Source(s)	Purpose(s) for collection	Disclosure to third parties
Identifiers , such as: Name, postal address, email address, IP address, identification numbers (e.g., social security number,	<ul style="list-style-type: none"> • Directly from consumers • Indirectly from consumers (e.g., from observing consumers’ actions on our Services) 	<ul style="list-style-type: none"> • To respond to consumers’ requests and inquiries • Communicate with consumers regarding our 	<ul style="list-style-type: none"> • Disclosure for business purposes to internet service providers, analytics providers, payment processors and warranty, insurance or service contract

<p>driver's license number, state identification number, military identification number or passport number)</p>	<ul style="list-style-type: none"> • Third-party service providers, including advertising companies, analytics providers, and websites or companies that provide information regarding vehicles or provide listings of vehicles available for sale/lease, that forward identifiers provided by consumers 	<p>products or services</p> <ul style="list-style-type: none"> • Enter into and process transactions with consumers • Send marketing communications • Complete government forms • Confirm consumers' identity and that they are at least 18 years old • Confirm consumers are licensed to drive our vehicles or take delivery of a vehicle purchased or leased from us 	<p>administrators, if applicable to transaction</p> <ul style="list-style-type: none"> • Disclosure for marketing purposes to advertising companies • Disclosure for safety and warranty purposes to vehicle manufacturer, if customer purchased/leased a new or certified vehicle or if their vehicle was serviced at our dealership • Disclosure to state or federal agencies, when required by law • Disclosure to vehicle manufacturer for marketing and analytical purposes, if customer purchased/leased a new or certified vehicle or if their vehicle was serviced at our dealership <i>[Note – if this bullet point is included, information sharing for this purpose amounts to a “sale” of information, and requires the dealer to have a “Do Not Sell My</i>
---	---	---	--

			<i>Information” button on its website – see Section II.]</i>
<p>Personal information categories listed in the California Customer Records statute (Cal. Civ. Code § 1798.80(e)), such as:</p> <p>Phone number; insurance information; bank account number, credit card number, debit card number, or other financial information, including information relating to consumers’ vehicle financing or lease terms, along with vehicle information; and/or signature(s).</p>	<ul style="list-style-type: none"> • Directly from consumers • Third-party service providers, including advertising companies and analytics providers 	<ul style="list-style-type: none"> • To respond to consumers’ requests and inquiries • Communicate with consumers regarding our products or services • Enter into and process transactions with consumers • Send marketing communications • Complete government forms • Confirm insurance coverage • Confirm identity • Obtain authorization to collect payments • Collect payments • Confirm acknowledgement of receipt of documents we provide to consumers 	<ul style="list-style-type: none"> • Disclosure for business purposes to internet service providers, delivery services and payment processors • State or federal agencies, when required by law • Disclosure to vehicle manufacturer for marketing and analytical purposes, if customer purchased/leased a new or certified vehicle or if their vehicle was serviced at our dealership [<i>Note – if this bullet point is included, information sharing for this purpose amounts to a “sale” of information, and requires the dealer to have a “Do Not Sell My Information” button on its website – see Section II.]</i>
Protected classification characteristics under	<ul style="list-style-type: none"> • Directly from consumers 	<ul style="list-style-type: none"> • To confirm identity • Confirm consumers are licensed to 	<ul style="list-style-type: none"> • Disclosure to manufacturer or lender for

<p>California or federal law, such as:</p> <p>A photocopy/scan of government issued identification reveals personal information. For example:</p> <ul style="list-style-type: none"> • Driver's license/state identification card - includes image, date of birth, physical description and gender • Permanent resident card - includes image, date and place of birth; • Social security card - includes social security number • Passport - includes image, date and place of birth and nationality • Military ID - includes image and rank <p>Completion of a Translated Contract Acknowledgement or signing of translated documents reveals a consumer's primary language</p>	<ul style="list-style-type: none"> • Government's Military Lending Act website 	<p>drive our vehicles or take delivery of a vehicle purchased or leased from us</p> <ul style="list-style-type: none"> • Confirm eligibility for a manufacturer or lender rebate and to apply for and process any such rebate • Determine coverage under the Military Lending Act in connection with a financed vehicle transaction • Provide consumers with copies of certain documents written in the language in which their finance or lease transaction was primarily negotiated, as required by law • Complete government forms 	<p>processing applicable rebate</p> <ul style="list-style-type: none"> • Disclosure to state or federal agencies, when required by law
<p>Commercial information, such as:</p>	<ul style="list-style-type: none"> • Directly from consumers 	<ul style="list-style-type: none"> • Enter into and process 	<ul style="list-style-type: none"> • Disclosure for business purposes to payment

Vehicle information, ownership information, and current lease or finance terms	<ul style="list-style-type: none"> • Third parties, such as vehicle manufacturer and/or advertising companies 	<p>transactions with consumers</p> <ul style="list-style-type: none"> • Appraise consumers' vehicles • Send informational and marketing communications • Retain records of transactions as required by law • Fulfill the terms of a written warranty or product recall • Process warranty, insurance or service contract claims • Share information with state agencies as required by law 	<p>processors, delivery services and warranty, insurance or service contract administrators, if applicable to transaction</p> <ul style="list-style-type: none"> • Disclosure for safety and warranty purposes to vehicle manufacturer, if customer purchased/leased a new or certified vehicle or if their vehicle was serviced at our dealership • Disclosure to state or federal agencies, when required by law
<p>Biometric information</p> <p>Consumers who finance/lease vehicles may be asked to complete a "Thumbprint form"</p>	<ul style="list-style-type: none"> • Directly from consumers 	<ul style="list-style-type: none"> • To confirm identity 	N/A
<p>Internet or other similar network activity information, such as:</p> <p>IP address, browsing history, and search history</p>	<ul style="list-style-type: none"> • Indirectly from consumers (e.g., from observing consumers' actions on our Services) 	<ul style="list-style-type: none"> • To communicate with consumers regarding our products and services • Improve user experiences by making our website easier to use and navigate, and more personalized based 	<ul style="list-style-type: none"> • Disclosure for business purposes to internet service providers

		on the profile we create about consumers	
Geolocation information , such as: IP address and vehicle location (using GPS, as permitted by law)	<ul style="list-style-type: none"> Indirectly from consumers (e.g., from observing consumers' actions on our Services) From vehicles equipped with GPS tracking (as permitted by law) 	<ul style="list-style-type: none"> To respond to consumers' requests and inquiries Enter into and process consumers' transactions with you Send marketing communications Track vehicles as permitted by law 	<ul style="list-style-type: none"> Disclosure for business purposes to internet service providers
Sensory data , such as Audio information from voicemail messages and/or recorded phone calls (with consumers' consent)	<ul style="list-style-type: none"> Directly from consumers 	<ul style="list-style-type: none"> To communicate with you; some phone calls are recorded (with your consent) for training our staff and for quality assurance purposes 	N/A
Professional or employment-related information , such as: Information regarding current occupation	<ul style="list-style-type: none"> Directly from consumers 	<ul style="list-style-type: none"> To confirm eligibility for a manufacturer or lender rebate and to apply for and process any such rebate To confirm eligibility for employee discount pricing Complete government forms, as required 	<ul style="list-style-type: none"> Disclosure to manufacturer or lender for processing applicable rebate Disclosure to state or federal agencies, when required by law
Non-public education information (per the Family Educational	<ul style="list-style-type: none"> Directly from consumers 	<ul style="list-style-type: none"> To confirm eligibility for a manufacturer or lender rebate and 	<ul style="list-style-type: none"> Disclosure to manufacturer or lender for

Rights and Privacy Act (20 U.S.C. Section 1232g, 34 C.F.R. Part 99)), such as: Information regarding whether a consumer is or will soon be a college graduate		to apply for and process any such rebate	processing applicable rebate
Inferences drawn from personal information to create a profile, such as: Information regarding consumers' vehicle preferences and needs	<ul style="list-style-type: none"> Indirectly from consumers (e.g., from observing consumers' actions on our Services) Third-party service providers, including advertising companies and analytics providers 	<ul style="list-style-type: none"> To market our products and services to consumers 	N/A

COOKIES

We, and third parties we allow, use cookies and other similar technologies. Cookies are small text files placed on your device that uniquely identify your device and which a website can transfer to a consumer's hard drive to keep records of his or her visit to a website. We, or third parties, may use session cookies or persistent cookies. Session cookies only last for the specific duration of your visit and are deleted when you close your browser. Persistent cookies remain on your device's hard drive until you delete them or they expire. Different cookies are used to perform different functions, which are explained below:

- **Essential.** Some cookies are essential in order to enable you to move around our website and use its features, such as accessing secure areas of our website. Without these cookies, we cannot enable appropriate content based on the type of device you are using.
- **Analytics.** We use Google Analytics to measure how you interact with our website and to improve your user experience. To learn more about Google Analytics privacy practices and opt-out mechanisms, please visit the Google Analytics Security and Privacy Principles page at <https://support.google.com/analytics/answer/6004245?hl=en>. Google also provides a complete privacy policy and instructions on opting-out of Google Analytics at <https://tools.google.com/dlpage/gaoptout>.

- **Targeted Advertising.** We use cookies to compile information on our users interaction with our website. We use this information to serve ads to you off of our website.

There are several ways to manage cookies. You can control the use of cookies at the browser level, by instructing your browser to accept cookies, disable cookies or notify you when receiving a new cookie. Please note that if you reject cookies, you may still use our website, but your ability to use some features or areas of our website may be limited. The Network Advertising Initiative also offers a means to opt-out of a number of advertising cookies. Please visit www.networkadvertising.org to learn more. Note that opting-out does not mean you will no longer receive online advertising. It does mean that the company or companies from which you opted-out will no longer deliver ads tailored to your preferences and usage patterns.

COLLECTION AND USE OF INFORMATION FROM CHILDREN

Our Services are not intended for children. We do not knowingly collect personal information from children, and none of our Services are designed to attract children. In the event that we learn that a person under the age of 13 has provided personal information to us, we will delete such personal information as soon as possible.

OPT-OUT

We provide you the opportunity to opt-out of marketing communications by clicking the “unsubscribe” link in email communications or by contacting us using the contact information provided below. We will process your request as soon as possible in accordance with applicable law, but please be aware that in some circumstances you may receive a few more messages until the unsubscribe is processed.

Additionally, we may send you information regarding our Services, such as information about changes to our policies and other notices and disclosures required by law. Generally, users cannot opt-out of these communications, but they will be primarily informational in nature, rather than promotional.

THIRD-PARTY LINKS

Our website contains links to other sites. DEALERSHIP is not responsible for the privacy practices or content of such other sites. If you have any questions about how these other sites use your information, you should review their policies and contact them directly.

YOUR CALIFORNIA PRIVACY RIGHTS

California Civil Code Section 1798.83 permits visitors to the Services who are California residents to request certain information, once a year, regarding our disclosure of personal information to third parties for their direct marketing purposes. To make such a request, please send us an email

using the contact information provided below and put “Shine the Light Request” in the subject line of your email.

From January 1, 2020, California consumers have the following rights:

- **Right to know**

You have the right to request information about the categories and specific pieces of personal information we have collected about you, as well as the categories of sources from which such information is collected, the purpose for collecting such information, and the categories of third parties with whom we share such information. Please see above.

You have the right to request information about our sale or disclosure for business purposes of your personal information to third parties in the preceding 12 months. Please see above.

- **Right to delete**

You have the right to request the deletion of your personal information. Please note that notwithstanding your request, California law permits us to retain certain categories of personal information for numerous purposes, including to complete a transaction, to perform a contract between you and DEALERSHIP, and to comply with a legal obligation.

- **Right to opt-out of sale**

You have the right to opt out of the sale of your personal information to third parties. You can exercise this right through the “Do Not Sell My Personal Information” link in the footer of our website, when such link becomes available on January 1, 2020.

[Note – if your dealership does not sell personal information, instead of the above language, state: “We do not and will not sell your personal information to third parties.”]

- **Right to non-discrimination**

You have the right to not be discriminated against for exercising any of these rights.

We do not sell or knowingly collect the personal information of minors under 16 years of age.

If you would like to exercise one or more of the rights above, please contact us using the contact information provided below. You may designate an authorized agent to make a request on your behalf. Such authorized agent must be registered with the California Secretary of State. We may deny a request from an agent that does not submit proof that they have been authorized by you to act on your behalf.

We may need to confirm your verifiable consumer request before completing your request, and, for example, may ask for you to confirm data points we already have about you. We will only use personal information provided in a verifiable consumer request to verify the requestor’s identity or authority to make the request.

We endeavor to respond to a verifiable consumer request within forty-five (45) days of its receipt. If we require more time, we will inform you of the reason and extension period in writing.

NOTICE REGARDING PUBLIC POSTING AREAS

Please note that any information you include in a message you post to any public posting area is available to anyone with Internet access. If you do not want people to know your email address, for example, do not include it in any message you post publicly. PLEASE BE EXTREMELY CAREFUL WHEN DISCLOSING ANY INFORMATION IN PUBLIC POSTING AREAS. DEALERSHIP IS NOT RESPONSIBLE FOR THE USE BY OTHERS OF THE INFORMATION THAT YOU DISCLOSE IN PUBLIC POSTING AREAS.

SECURITY

We implement reasonable security measures to ensure the security of your personal information. Please understand, however, that no data transmissions over the Internet can be guaranteed to be 100% secure. Consequently, DEALERSHIP cannot ensure or warrant the security of any information you transmit to us and you understand that any information that you transfer to us is done at your own risk. If we learn of a security systems breach we may attempt to notify you electronically so that you can take appropriate protective steps. By using the Services or providing personal information to us, you agree that we can communicate with you electronically regarding security, privacy and administrative issues relating to your use of the Services. We may post a notice via our website if a security breach occurs. We may also send an email to you at the email address you have provided to us in these circumstances. Depending on where you live, you may have a legal right to receive notice of a security breach in writing.

INTERNATIONAL DATA TRANSFERS

DEALERSHIP is based in the U.S. If you choose to provide us with information, please understand that your personal information may be transferred to the U.S. and that we may transfer that information to our affiliates and subsidiaries or to other third parties, across borders, and from your country or jurisdiction to other countries or jurisdictions around the world. If you are visiting from the EU or other regions with laws governing data collection and use that may differ from U.S. law, please note that you are transferring your personal information to the U.S. and other jurisdictions which may not have the same data protection laws as the EU. We put in place appropriate operational, procedural and technical measures in order to ensure the protection of your personal information. You acknowledge you understand that by providing your personal information: (i) your personal information will be used for the uses identified above in accordance with this Policy; and (ii) your personal information may be transferred to the U.S. and other jurisdictions as indicated above, in accordance with applicable law.

ASSIGNMENT

In the event that all or part of our assets are sold or acquired by another party, or in the event of a merger, you grant us the right to assign the personal information collected via the Services.

DISPUTE RESOLUTION AND AGREEMENT TO ARBITRATE

Except where and to the extent prohibited by law, by using the Services, you and DEALERSHIP agree that, if there is any controversy, claim, action, or dispute arising out of or related to your use of the Services or the breach, enforcement, interpretation, or validity of this Policy or any part of it (“Dispute”), both parties shall first try in good faith to settle such Dispute by providing written notice to the other party describing the facts and circumstances of the Dispute and allowing the receiving party thirty (30) days in which to respond to or settle the Dispute. Notice shall be sent to:

- DEALERSHIP, at [INSERT ADDRESS] or
- You, at the address we have on file for you.

Both you and DEALERSHIP agree that this dispute resolution procedure is a condition precedent that must be satisfied before initiating any litigation or filing any claim against the other party. IF ANY DISPUTE CANNOT BE RESOLVED BY THE ABOVE DISPUTE RESOLUTION PROCEDURE, YOU AGREE THAT THE SOLE AND EXCLUSIVE JURISDICTION FOR SUCH DISPUTE WILL BE DECIDED BY BINDING ARBITRATION ON AN INDIVIDUAL BASIS. ARBITRATION ON AN INDIVIDUAL BASIS MEANS THAT YOU WILL NOT HAVE, AND YOU WAIVE THE RIGHT FOR A JUDGE OR JURY TO DECIDE YOUR CLAIMS, AND THAT YOU MAY NOT PROCEED IN A CLASS, CONSOLIDATED, OR REPRESENTATIVE CAPACITY. Other rights that you and we would otherwise have in court will not be available, or will be more limited in arbitration, including discovery and appeal rights. All such disputes shall be exclusively submitted to [INSERT NAME OF ARBITRATION SERVICE AND WEBSITE ADDRESS OR EMAIL ADDRESS] for binding arbitration under its rules then in effect, before one arbitrator to be mutually agreed upon by both parties.

The arbitrator, and not any federal, state, or local court or agency, shall have exclusive authority to resolve any dispute arising under or relating to the interpretation, applicability, enforceability, or formation of this Policy, including any claim that all or any part of this Policy is void or voidable.

OTHER ARBITRATION AGREEMENTS

In the event of a conflict between this agreement to arbitrate and any other arbitration agreement between you and the DEALERSHIP, such as an arbitration agreement contained in a retail installment sale contract, lease agreement, or repair estimate (Other Arbitration Agreement), the terms of the Other Arbitration Agreement shall govern and prevail in each instance.

CHOICE OF LAW

This Policy has been made in and shall be construed in accordance with the laws of the State of California, without giving effect to any conflict of law principles. Any disputes or claims not subject to the arbitration provision discussed above shall be resolved by a court located in the State of California and you agree and submit to the exercise of personal jurisdiction of such courts for the purpose of litigating any such claim or action.

HOW WE RESPOND TO DO-NOT-TRACK SIGNALS

We treat user-enabled privacy controls, such as a browser plugin or privacy setting, that communicates or signals the consumer's choice to opt-out of the sale of their personal information, as a valid request to opt-out.

CHANGES TO THIS PRIVACY POLICY

We reserve the right to change this Policy from time to time. When we do, we will also revise the "Effective Date" at the top of this Policy. If we make material changes to the Policy, we will notify you by placing a prominent notice on our website and/or by sending you an email at the email address we have on file for you. We encourage you to periodically review this Policy to keep up to date on how we are handling your personal information.

ADDITIONAL FORMATS, ACCESSABILITY AND LANGUAGES

Click **here** [insert link] to print a copy of our Notice at Collection of Personal Information.

Click **here** [insert link] to print a copy of this Privacy Policy.

Those with disabilities may access our Notice at Collection of Personal Information in an alternate format by clicking **here** [insert link].

Those with disabilities may access this Privacy Policy in an alternate format by clicking **here** [insert link].

In addition to English, our Notice at Collection of Personal Information is available in the following languages: [insert languages and a link for each].

In addition to English, this Privacy Policy is available in the following languages: [insert languages and a link for each].

CONTACT US

If you have any questions, comments or concerns about our privacy practices or this Policy, please contact us at:

[INSERT CONTACT INFORMATION, I.E., ADDRESS, EMAIL ADDRESS AND PHONE NUMBER]



D. Sample Privacy Notice

In 2010, federal regulators released an Online Form Builder that businesses can download and use to develop and print customized versions of a model consumer privacy notice. (See https://www.federalreserve.gov/bankinfo/reg/privacy_notice_instructions.pdf.) There are six different Model Privacy Notice forms for dealers to choose from based on their privacy practices. The sample below is based on Model Form 4, intended for dealerships that have affiliates, but do not share their customers' credit-related information with affiliates or share any NPI with nonaffiliates for marketing purposes. When choosing a Privacy Notice, be sure to select the appropriate form and customize it based on your dealership's actual privacy practices.

Rev. 1/2020

FACTS		WHAT DOES [DEALERSHIP] DO WITH YOUR PERSONAL INFORMATION?	
Why?	Financial companies choose how they share your personal information. Federal law gives consumers the right to limit some but not all sharing. Federal law also requires us to tell you how we collect, share, and protect your personal information. Please read this notice carefully to understand what we do.		
What?	<p>The types of personal information we collect and share depend on the product or service you have with us. This information can include:</p> <ul style="list-style-type: none"> ▪ Social Security number and income ▪ Credit history and credit scores ▪ Employment information and checking account information <p>When you are <i>no longer</i> our customer, we continue to share your information as described in this notice.</p>		
How?	All financial companies need to share customers' personal information to run their everyday business. In the section below, we list the reasons financial companies can share their customers' personal information; the reasons [Dealership] chooses to share; and whether you can limit this sharing.		
Reasons we can share your personal information		Does [Dealership] share?	Can you limit this sharing?
For our everyday business purposes— such as to process your transactions, maintain your account(s), respond to court orders and legal investigations, or report to credit bureaus		Yes	No
For our marketing purposes— to offer our products and services to you		Yes	No
For joint marketing with other financial companies		Yes	No
For our affiliates' everyday business purposes— information about your transactions and experiences		Yes	No
For our affiliates' everyday business purposes— information about your creditworthiness		No	We do not share
For nonaffiliates to market to you		No	We do not share
Questions?	Call [insert title] at () - -		

Page 2

Who we are	
Who is providing this notice?	[Dealership Corporate/LLC name] is doing business as [Dealership fictitious name].
What we do	
How does [Dealership] protect my personal information?	To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings.
How does [Dealership] collect my personal information?	<p>We collect your personal information, for example, when you</p> <ul style="list-style-type: none"> ▪ Complete a credit application ▪ Apply for financing or for a lease ▪ Provide employment information ▪ Give us your contact information ▪ Show your driver's license <p>We also collect your personal information from others, such as credit bureaus, affiliates, or other companies.</p>
Why can't I limit all sharing?	<p>Federal law gives you the right to limit only</p> <ul style="list-style-type: none"> ▪ sharing for affiliates' everyday business purposes—information about your creditworthiness ▪ affiliates from using your information to market to you ▪ sharing for nonaffiliates to market to you <p>State laws and individual companies may give you additional rights to limit sharing.</p>
Definitions	
Affiliates	<p>Companies related by common ownership or control. They can be financial and nonfinancial companies.</p> <ul style="list-style-type: none"> ▪ Our affiliates include [insert names here]
Nonaffiliates	<p>Companies not related by common ownership or control. They can be financial and nonfinancial companies.</p> <ul style="list-style-type: none"> ▪ [Dealership] does not share with nonaffiliates so they can market to you.
Joint marketing	<p>A formal agreement between nonaffiliated financial companies that together market financial products or services to you.</p> <ul style="list-style-type: none"> ▪ [Dealership] engages in joint marketing with banks, credit unions, and finance lenders.
Other important information	
<p>To provide you with additional information regarding our privacy practices and your rights under the California Consumer Privacy Act, a copy of our Notice at Collection of Personal Information has been made available to you. Our Privacy Policy may be accessed at [URL]. By signing below, you acknowledge receipt of this Privacy Notice.</p>	
 _____ Signature	 _____ Signature
_____ Date	_____ Date
_____ Print Name	_____ Print Name

E. Sample In-Person Data Request Form

[DEALERSHIP]
REQUESTS UNDER THE CALIFORNIA CONSUMER PRIVACY ACT

[Check A or B below]

- ☐ A. [Dealership] does not and will not sell your personal information to third parties.
☐ B. You have the right to opt out of the sale of your personal information to third parties.

If you are a California resident, as of January 1, 2020 you have the following rights relating to your personal information:

1. You have the right to submit a Request to Know information about the categories and specific pieces of personal information we have collected about you, as well as the categories of sources from which such information is collected, the purpose for collecting such information, the categories of third parties with whom we share such information and the purpose for which it was shared.
2. You have the right to submit a Request to Delete your personal information. Please note that notwithstanding your request, California law permits us to retain certain categories of personal information for numerous purposes, including to complete a transaction, to perform a contract between you and the dealership, and to comply with a legal obligation, such as a record retention requirement.
3. If box B above is checked, you have the right submit a Request to Opt-out of the sale of your personal information to third parties.

To exercise one or more of the these rights, complete the request form below:

Consumer Contact Information	Data Request
Name:	<input type="checkbox"/> Request to Know Categories of Personal Information Collected
Email:	<input type="checkbox"/> Request to Know Specific Pieces of Personal Information Collected
Address:	<input type="checkbox"/> Request to Delete Personal Information
Phone number:	<input type="checkbox"/> Request to Opt-Out (if box B above is checked)
Phone number:	Date of Request:

If you have submitted a Request to Know information, we will process your request by providing the information described above within 45 days (unless additional time is needed, in which case we will notify you regarding the delay).

If you have submitted a Request to Delete information, we will process your request by deleting your information, unless we are permitted or required to retain it. We will discontinue marketing to you and we will provide a written response regarding your request within 45 days (unless additional time is needed, in which case we will notify you regarding the delay).

If you have submitted a Request to Opt-Out (if box B above is checked), within 15 days we will notify all third parties to whom we have sold your personal information within the past 90 days and instruct them not to further sell your information. We will notify you when this has been completed.

- ☐ Requester's identification verified by unexpired California driver's license or California ID.

 Dealership Representative

F. Sample Initial Response to Data Request

[DEALERSHIP]
INITIAL RESPONSE TO DATA REQUEST

[Check A or B below]

- ☐ A. [Dealership] does not and will not sell your personal information to third parties.
☐ B. You have the right to opt out of the sale of your personal information to third parties.

On _____, we received the following data request made by you or on your behalf, pursuant to the California Consumer Privacy Act (CCPA):

- ☐ **Request to Know** information. After we have verified your identity, we will process your request by providing information about the categories and/or specific pieces of personal information we have collected about you, as well as the categories of sources from which such information is collected, the purpose for collecting such information, the categories of third parties with whom we share such information and the purpose for which it was shared. If box B above is checked, we will provide the categories of third parties to whom we have sold your information and the business purpose for which it was sold. We will provide this response within 45 days of the above date, unless additional time is needed, in which case we will notify you regarding the delay.
- ☐ **Request to Delete** ☐ portions or ☐ all of your information. After we have verified your identity, we will process your request by deleting your information pursuant to your request, unless we are permitted or required to retain it. Please note that notwithstanding your request, California law permits us to retain certain categories of personal information for numerous purposes, including to complete a transaction, to perform a contract between you and the dealership, and to comply with a legal obligation, such as a record retention requirement. We will provide a response to your request for deletion within 45 days of the above date, unless additional time is needed, in which case we will notify you regarding the delay.
- ☐ **Request to Opt-Out** of the sale of your information. If box A above is checked, we will not provide a further response and will consider your request to be completed. If box B above is checked, after we have verified your identity, within 15 days we will notify all third parties to whom we have sold your personal information within the past 90 days and instruct them not to further sell your information. We will notify you when this has been completed.

Verification of Your Identity

- ☐ We have verified your identity; no further action is required.
☐ Two-factor identification is required. We will either send an email to the email address you previously used to interact with us and/or call you using the phone number you previously used to interact with us.
☐ Because you have requested the specific pieces of personal information we have collected about you, you must meet with the CCPA Manager at our dealership and present your California driver's license or identification card and submit a declaration under penalty of perjury stating that you are the consumer whose personal information is being requested. When you contact us, you will be provided with further instructions regarding this requirement.

G. Sample Responses to Deletion Requests

Below are three templates for responding to deletion requests. The templates vary based on the consumer's interaction with the dealership. The forms increase in length depending on whether the consumer is merely a "window shopper," has applied for credit, or has purchased products or service from the dealership. Your dealership may want to use only the longest and most comprehensive form for all deletion requests, similar to Template (iii) / Form RTD C, or you may want to use a variety of forms similar to these three samples:

- Template (i) **Consumer only visited** the dealership or its website, but did not apply for credit, purchase/lease a vehicle, buy parts or obtain repair services pursuant to a parts ticket or repair order (Form RTD A);
- Template (ii) Consumer **applied for credit**, but did not purchase/lease a vehicle, buy parts or obtain repair services pursuant to a parts ticket or repair order (Form RTD B);
- Template (iii) Consumer **purchased/leased a vehicle, bought parts and/or obtained repair services** pursuant to a parts ticket or repair order (Form RTD C).

Template (i): this sample form is intended for consumers who visited the dealership or its website, but did not apply for credit, purchase/lease a vehicle, or buy parts or obtain repair services pursuant to a parts ticket or repair order. Note that all deletion requests require a secondary confirmation prior to deleting the information.

**RESPONSE TO REQUEST TO DELETE PERSONAL INFORMATION
UNDER THE CALIFORNIA CONSUMER PRIVACY ACT**

To: [Name of Requester]

Date of receipt of request: _____

Date of response: _____

[Name of Dealership] ("Dealership," "we," "us" or "our") respects the privacy of the information our customers entrust to us. We received a request to delete personal information* made by you or on your behalf pursuant to the California Consumer Privacy Act (CCPA).

Response to Request

- ☐ We are unable to locate in our records any personal information relating to you.
- ☐ We are unable to confirm your identity. Your request to delete personal information is denied. We will treat your request as a request to opt-out of selling your personal information.
- ☐ Your request is deficient because it was not submitted through one of the designated methods or it is deficient in some other manner unrelated to the verification process. Enclosed with this response are directions on how to submit the request or remedy any deficiencies with the request.
- ☐ We have processed your request by deleting information that is not subject to an exception. Such data was deleted by:
- ☐ permanently and completely erasing the personal information on our existing systems with the exception of archived or back-up systems;
 - ☐ de-identifying the personal information; or
 - ☐ aggregating the personal information.

We have also notified third-parties with whom your data has been shared to delete any information that is not subject to an exception.

The Dealership will maintain a record of your request pursuant to Civil Code Section 1798.105(d).

For more information regarding our privacy practices and your rights under the California Consumer Privacy Act, view our Privacy Policy at [\[insert URL for Privacy Policy\]](#).

*"Personal information" does not include the following items, which are therefore not subject to deletion:

- Publicly available information, defined as information lawfully made available from federal, state, or government records;
- Protected health information;
- The sale of information to or from a consumer reporting agency for use in a consumer report;
- Personal information about a job applicant or a business' employees (excluded from most provisions of the CCPA through December 31, 2020);
- Personal information provided in the context of a business to business communication/transaction (excluded through December 31, 2020);
- Personal information collected, processed, sold or disclosed pursuant to the Gramm-Leach-Bliley Act;
- Personal information collected, processed, sold or disclosed pursuant to the Driver's Privacy Protection Act of 1994

(Rev 1/2020) Form RTD A

Template (ii): this sample form is intended for consumers who applied for credit, but did not purchase/lease a vehicle, buy parts or obtain repair services pursuant to a parts ticket or repair order. Note that all deletion requests require a secondary confirmation prior to deleting the information.

**RESPONSE TO REQUEST TO DELETE PERSONAL INFORMATION
UNDER THE CALIFORNIA CONSUMER PRIVACY ACT**

To: [Name of Requester]

Date of receipt of request: _____

Date of response: _____

[Name of Dealership] ("Dealership," "we," "us" or "our") respects the privacy of the information our customers entrust to us. We received a request to delete personal information* made by you or on your behalf pursuant to the California Consumer Privacy Act.

Response to Request

- ☐ We are unable to confirm your identity. Your request to delete personal information is denied. We will treat your request as a request to opt-out of selling your personal information.
- ☐ Your request is deficient because it was not submitted through one of the designated methods or it is deficient in some other manner unrelated to the verification process. Enclosed with this response are directions on how to submit the request or remedy any deficiencies with the request.
- ☐ We have processed your request by deleting information that is not subject to an exception (see below). Such data was deleted by:
- ☐ permanently and completely erasing the personal information on our existing systems with the exception of archived or back-up systems;
 - ☐ de-identifying the personal information; or
 - ☐ aggregating the personal information.

We have also notified third-parties with whom your data has been shared to delete any information that is not subject to an exception.

Exceptions to Requests for Deletion

Although portions of your data will not be deleted at this time, we will remove your contact information from our marketing lists. We will retain portions of your data for the reasons that are checked below:

Statute(s) or regulation(s) requiring that we maintain documentation:

- ☐ Credit applications by consumers who do not purchase or lease a vehicle from the Dealership must be retained for 25 months (12 Code of Federal Regulations § 202.12(b))
- ☐ Other: _____
- ☐ Other: _____

- ☐ To defend against potential legal claims, we retain records for the period of time set forth in our records retention schedule.

The Dealership will maintain a record of your request pursuant to Civil Code Section 1798.105(d).

For more information regarding our privacy practices and your rights under the California Consumer Privacy Act, view our Privacy Policy at [\[insert URL for Privacy Policy\]](#).

*“Personal information” does not include the following items, which are therefore not subject to deletion:

- Publicly available information, defined as information lawfully made available from federal, state, or government records;
- The sale of information to or from a consumer reporting agency for use in a consumer report;
- Personal information about a job applicant or a business’ employees (excluded from most provisions of the CCPA through December 31, 2020);
- Personal information provided in the context of a business to business communication/transaction (excluded through December 31, 2020);
- Personal information collected, processed, sold or disclosed pursuant to the Gramm-Leach-Bliley Act
- Personal information collected, processed, sold or disclosed pursuant to the Driver’s Privacy Protection Act of 1994

(Rev 1/2020) Form RTD B

Template (iii): this sample form is intended for consumers who purchased/leased a vehicle, bought parts and/or obtained repair services pursuant to a parts ticket or repair order. Note that all deletion requests require a secondary confirmation prior to deleting the information.

RESPONSE TO REQUEST TO DELETE PERSONAL INFORMATION UNDER THE CALIFORNIA CONSUMER PRIVACY ACT

To: [Name of Requester]

Date of receipt of request: _____

Date of response: _____

[Name of Dealership] ("Dealership," "we," "us" or "our") respects the privacy of the information our customers entrust to us. We received a request to delete personal information* made by you or on your behalf pursuant to the California Consumer Privacy Act (CCPA).

Response to Request

- ☐ We are unable to confirm your identity. Your request to delete personal information is denied. We will treat your request as a request to opt-out of selling your personal information.
- ☐ Your request is deficient because it was not submitted through one of the designated methods or it is deficient in some other manner unrelated to the verification process. Enclosed with this response are directions on how to submit the request or remedy any deficiencies with the request.
- ☐ We have processed your request by deleting information that is not subject to an exception (see below). Such data was deleted by:
 - ☐ permanently and completely erasing the personal information on our existing systems with the exception of archived or back-up systems;
 - ☐ de-identifying the personal information; or
 - ☐ aggregating the personal information.

We have also notified third-parties with whom your data has been shared to delete any information that is not subject to an exception.

Exceptions to Requests for Deletion

Although portions of your data will not be deleted at this time, we will remove your contact information from our marketing lists. We will retain portions of your data for the reasons that are checked below:

- ☐ **To complete a transaction.** Personal information is not deleted because it is needed to complete a transaction for which it was collected; provide a good or service requested by you or reasonably anticipated within the context of an ongoing business relationship with you; or otherwise perform a contract between us and you.
- ☐ **To fulfill the terms of a written warranty or provide notification of a product recall** conducted in accordance with federal law.

☐ **For certain internal uses.** Personal information is not deleted because it is needed solely for internal use in a lawful manner that is compatible with the context in which the information was provided.

☐ **To comply with a legal obligation.** Personal information is not deleted because it is needed to comply with the following legal obligation(s):

Statute(s) or regulation(s) requiring that we maintain documentation:

- ☐ All pertinent records directly concerned with vehicle sale or lease transactions must be retained for 3 years (13 California Code of Regulations § 272.00)
- ☐ Odometer disclosure statements must be retained for 5 years (49 Code of Federal Regulations § 580.8)
- ☐ Conditional sale contracts must be retained for 7 years (Civil Code § 2984.5)
- ☐ For financed transactions, documents relating to credit worthiness must be retained for 7 years (Civil Code § 2984.5)
- ☐ Credit applications by consumers who do not purchase or lease a vehicle from the Dealership must be retained for 25 months (12 Code of Federal Regulations § 202.12(b))
- ☐ Vehicle service records must be retained for 3 years (Business and Professions Code § 9884.11)
- ☐ Other: _____
- ☐ Other: _____

☐ To defend against potential legal claims, we retain records for the period of time set forth in our records retention schedule.

The Dealership will maintain a record of your request pursuant to Civil Code Section 1798.105(d).

For more information regarding our privacy practices and your rights under the California Consumer Privacy Act, view our Privacy Policy at [\[insert URL for Privacy Policy\]](#).

*“Personal information” does not include the following items, which are therefore not subject to deletion:

- Publicly available information, defined as information lawfully made available from federal, state, or government records;
- Protected health information;
- The sale of information to or from a consumer reporting agency for use in a consumer report;
- Personal information about a job applicant or a business’ employees (excluded from most provisions of the CCPA through December 31, 2020);
- Personal information provided in the context of a business to business communication/transaction (excluded through December 31, 2020);
- Personal information collected, processed, sold or disclosed pursuant to the GLBA;
- Personal information collected, processed, sold or disclosed pursuant to the Driver’s Privacy Protection Act of 1994

(Rev 1/2020) Form RTD C

H. Sample Responses to Right to Know Requests

Below are three templates for responding to Right to Know Requests regarding categories of personal information. The sample templates are designed to reflect the level of interaction with the consumer. Your dealership may want to use a form similar to the longest and most comprehensive form for all deletion requests (Template (iii) /Form RTK C), or you may want to use a variety of forms similar to these three samples:

- Template (i) **Consumer only visited** the dealership or its website, but did not apply for credit; purchase/lease a vehicle, buy parts or obtain repair services (Form RTK A);
- Template (ii) Consumer **applied for credit**, but did not purchase/lease a vehicle, buy parts or obtain repair services (Form RTK B);
- Template (iii) Consumer **purchased/leased a vehicle, bought parts and/or obtained repair services** (Form RTK C).

Also included is Template (iv), a sample response to a consumer who requests to know the **specific pieces** of personal information that have been collected.

Template (i): this sample form is intended for consumers who visited the dealership or its website, but did not apply for credit, purchase/lease a vehicle, or buy parts or obtain repair services pursuant to a parts ticket or repair order.

**RESPONSE TO REQUEST TO KNOW ABOUT CATEGORIES OF INFORMATION COLLECTED
UNDER THE CALIFORNIA CONSUMER PRIVACY ACT**

To: [Name of Requester]

Date of receipt of request: _____

Date of response: _____

[Name of Dealership] (“Dealership,” “we,” “us” or “our”) respects the privacy of the information our customers entrust to us. This is our response to your request to know information about the following items under the California Consumer Privacy Act (CCPA):

- Categories of personal information collected;
- Categories of sources from which the personal information was collected;
- Business or commercial purposes for collecting or selling the personal information;
- Categories of third parties with whom the business shared or sold the personal information;
- Business or commercial purpose for which it sold or disclosed the personal information.

Under the CCPA, “Personal information” does not include the following items, which may be excluded from this response:

- Publicly available information, defined as information lawfully made available from federal, state, or government records;
- Protected health information;
- The sale of information to or from a consumer reporting agency for use in a consumer report;
- Personal information about a job applicant or a business’ employees (excluded from most provisions of the CCPA through December 31, 2020);
- Personal information provided in the context of a business to business communication/transaction (excluded through December 31, 2020);
- Personal information collected, processed, sold or disclosed pursuant to the Gramm-Leach-Bliley Act ;
- Personal information collected, processed, sold or disclosed pursuant to the Driver’s Privacy Protection Act of 1994

Response to Request

- ☐ We are unable to locate in our records any personal information relating to you.
- ☐ We are unable to confirm your identity. Your request to know the categories of personal information collected is denied.
- ☐ The chart below reflects the information we have collected about you during the past 12 months.

Category of personal data	Source(s)	Purpose(s)	Disclosure to third parties
<input type="checkbox"/> Identifiers , such as: Name, postal address, email address, IP address,	<input type="checkbox"/> Directly from you <input type="checkbox"/> Indirectly from you (e.g., from observing actions on our Services)	<input type="checkbox"/> To respond to your requests and inquiries	<input type="checkbox"/> Disclosure for business purposes to internet service providers, analytics providers

identification numbers (e.g., social security number, driver's license number, state identification number, military identification number or passport number)	<input type="checkbox"/> Third-party service providers, including advertising companies, analytics providers, and websites or companies that provide information regarding vehicles or provide listings of vehicles available for sale/lease, that forward identifiers provided by you	<input type="checkbox"/> Communicate with you regarding our products or services <input type="checkbox"/> Enter into transactions with you <input type="checkbox"/> Send marketing communications <input type="checkbox"/> Confirm your identity and that you are at least 18 years old <input type="checkbox"/> Confirm you are licensed to drive our vehicles	<input type="checkbox"/> Disclosure for marketing purposes to advertising companies
<input type="checkbox"/> Personal information categories listed in the California Customer Records statute (Cal. Civ. Code § 1798.80(e)), such as: Phone number	<input type="checkbox"/> Directly from you <input type="checkbox"/> Third-party service providers, including advertising companies and analytics providers	<input type="checkbox"/> To respond to your requests and inquiries <input type="checkbox"/> Communicate with you regarding our products or services <input type="checkbox"/> Send marketing communications	<input type="checkbox"/> Disclosure for business purposes to internet service providers and payment processors
<input type="checkbox"/> Protected classification characteristics under California or federal law, such as: A photocopy/scan of government issued identification reveals personal information. For example: <ul style="list-style-type: none"> • Driver's license/state identification card - includes image, date of birth, physical description and gender • Permanent resident card - includes image, date and place of birth; • Social security card - includes social security number • Passport - includes image, date and place of birth and nationality • Military ID - includes image and rank 	<input type="checkbox"/> Directly from you	<input type="checkbox"/> To confirm identity <input type="checkbox"/> Confirm you are licensed to drive our vehicles <input type="checkbox"/> Confirm eligibility for a manufacturer or lender rebate and to apply for and process any such rebate	N/A
<input type="checkbox"/> Commercial information, such as:	<input type="checkbox"/> Directly from you <input type="checkbox"/> Third parties, such as vehicle manufacturer and/or advertising companies	<input type="checkbox"/> Appraise your vehicle <input type="checkbox"/> Send informational and marketing communications	N/A

Vehicle information, ownership information, and current lease or finance terms			
<input type="checkbox"/> Internet or other similar network activity information , such as: IP address, browsing history, and search history	<input type="checkbox"/> Indirectly from you (e.g., from observing your actions on our Services)	<input type="checkbox"/> To communicate with you regarding our products and services <input type="checkbox"/> Improve user experiences by making our website easier to use and navigate, and more personalized based on the profile we create about you	<input type="checkbox"/> Disclosure for business purposes to internet service providers
<input type="checkbox"/> Geolocation information , such as: IP address	<input type="checkbox"/> Indirectly from you (e.g., from observing your actions on our Services)	<input type="checkbox"/> To respond to your requests and inquiries <input type="checkbox"/> Send marketing communications	<input type="checkbox"/> Disclosure for business purposes to internet service providers
<input type="checkbox"/> Sensory data , such as Audio information from voicemail messages and/or recorded phone calls (with your consent)	<input type="checkbox"/> Directly from you	<input type="checkbox"/> To communicate with you; some phone calls are recorded (with your consent) for training our staff and for quality assurance purposes	N/A
<input type="checkbox"/> Professional or employment-related information , such as: Information regarding current occupation	<input type="checkbox"/> Directly from you	<input type="checkbox"/> To confirm eligibility for a manufacturer or lender rebate, if applicable <input type="checkbox"/> To confirm eligibility for employee discount pricing	N/A
<input type="checkbox"/> Non-public education information (per the Family Educational Rights and Privacy Act (20 U.S.C. Section 1232g, 34 C.F.R. Part 99)) , such as: Information regarding whether you were or would soon be a college graduate	<input type="checkbox"/> Directly from you	<input type="checkbox"/> To confirm eligibility for a manufacturer or lender rebate, if applicable	N/A
<input type="checkbox"/> Inferences drawn from personal information to create a profile , such as: Information regarding your vehicle preferences and needs	<input type="checkbox"/> Indirectly from you (e.g., from observing your actions on our Services) <input type="checkbox"/> Third-party service providers, including advertising companies and analytics providers	<input type="checkbox"/> To market our products and services to you	N/A

For more information regarding our privacy practices and your rights under the California Consumer Privacy Act, view our Privacy Policy at [\[insert URL for Privacy Policy\]](#).

(Rev 1/2020) Form RTK A

Template (ii): this sample form is intended for consumers who applied for credit, but did not purchase/lease a vehicle, buy parts or obtain repair services pursuant to a parts ticket or repair order.

**RESPONSE TO REQUEST TO KNOW ABOUT CATEGORIES OF INFORMATION COLLECTED
UNDER THE CALIFORNIA CONSUMER PRIVACY ACT**

To: [Name of Requester]

Date of receipt of request : _____

Date of response to request: _____

[Name of Dealership] ("Dealership," "we," "us" or "our") respects the privacy of the information our customers entrust to us. This is our response to your request to know information about the following items under the California Consumer Privacy Act (CCPA):

- Categories of personal information collected;
- Categories of sources from which the personal information was collected;
- Business or commercial purposes for collecting or selling the personal information;
- Categories of third parties with whom the business shared or sold the personal information;
- Business or commercial purpose for which it sold or disclosed the personal information.

Under the CCPA, "Personal information" does not include the following items, which may be excluded from this response:

- Publicly available information, defined as information lawfully made available from federal, state, or government records;
- Protected health information;
- The sale of information to or from a consumer reporting agency for use in a consumer report;
- Personal information about a job applicant or a business' employees (excluded from most provisions of the CCPA through December 31, 2020);
- Personal information provided in the context of a business to business communication/transaction (excluded through December 31, 2020);
- Personal information collected, processed, sold or disclosed pursuant to the Gramm-Leach-Bliley Act;
- Personal information collected, processed, sold or disclosed pursuant to the Driver's Privacy Protection Act of 1994

Check A. or B. below

A. ☐ We are unable to confirm your identity. Your request to know about categories of personal information collected is denied.

B. ☐ The chart below reflects the information we have collected about you during the past 12 months.

Category of personal data	Source(s)	Purpose(s)	Disclosure to third parties
<input type="checkbox"/> Identifiers , such as:	<input type="checkbox"/> Directly from you	<input type="checkbox"/> To respond to your requests and inquiries	<input type="checkbox"/> Disclosure for business purposes to internet service

Name, postal address, email address, IP address, identification numbers (e.g., social security number, driver's license number, state identification number, military identification number or passport number)	<input type="checkbox"/> Indirectly from you (e.g., from observing actions on our Services) <input type="checkbox"/> Third-party service providers, including advertising companies, analytics providers, and websites or companies that provide information regarding vehicles or provide listings of vehicles available for sale/lease, that forward identifiers provided by you	<input type="checkbox"/> Communicate with you regarding our products or services <input type="checkbox"/> Enter into and process transactions with you <input type="checkbox"/> Send marketing communications <input type="checkbox"/> Confirm your identity and that you are at least 18 years old <input type="checkbox"/> Confirm you are licensed to drive our vehicles	providers and analytics providers <input type="checkbox"/> Disclosure for marketing purposes to advertising companies
<input type="checkbox"/> Personal information categories listed in the California Customer Records statute (Cal. Civ. Code § 1798.80(e)), such as: Phone number; insurance information; bank account number, credit card number, debit card number, or other financial information, including information relating to your vehicle financing or lease terms, along with vehicle information; and/or signature(s).	<input type="checkbox"/> Directly from you <input type="checkbox"/> Third-party service providers, including advertising companies and analytics providers	<input type="checkbox"/> To respond to your requests and inquiries <input type="checkbox"/> Communicate with you regarding our products or services <input type="checkbox"/> Enter into transactions with you <input type="checkbox"/> Send marketing communications <input type="checkbox"/> Confirm identity <input type="checkbox"/> Confirm acknowledgement of receipt of documents we provide to you	<input type="checkbox"/> Disclosure for business purposes to internet service providers
<input type="checkbox"/> Protected classification characteristics under California or federal law, such as: A photocopy/scan of government issued identification reveals personal information. For example: <ul style="list-style-type: none"> • Driver's license/state identification card - includes image, date of birth, physical description and gender • Permanent resident card - includes image, date and place of birth; • Social security card - includes social security number • Passport - includes image, date and place of birth and nationality 	<input type="checkbox"/> Directly from you <input type="checkbox"/> Government's Military Lending Act website	<input type="checkbox"/> To confirm identity <input type="checkbox"/> Confirm you are licensed to drive our vehicles Confirm eligibility for a manufacturer or lender rebate and to apply for and process any such rebate <input type="checkbox"/> Determine coverage under the Military Lending Act in connection with a financed vehicle transaction	<input type="checkbox"/> Disclosure to manufacturer or lender for processing applicable rebate

<ul style="list-style-type: none"> • Military ID - includes image and rank 			
<input type="checkbox"/> Commercial information , such as: Vehicle information, ownership information, and current lease or finance terms	<input type="checkbox"/> Directly from you <input type="checkbox"/> Third parties, such as vehicle manufacturer and/or advertising companies	<input type="checkbox"/> Appraise your vehicle <input type="checkbox"/> Send informational and marketing communications	N/A
<input type="checkbox"/> Biometric information You completed a "Thumbprint form"	<input type="checkbox"/> Directly from you	<input type="checkbox"/> To confirm identity	N/A
<input type="checkbox"/> Internet or other similar network activity information , such as: IP address, browsing history, and search history	<input type="checkbox"/> Indirectly from you (e.g., from observing your actions on our Services)	<input type="checkbox"/> To communicate with you regarding our products and services <input type="checkbox"/> Improve user experiences by making our website easier to use and navigate, and more personalized based on the profile we create about you	<input type="checkbox"/> Disclosure for business purposes to internet service providers
<input type="checkbox"/> Geolocation information , such as: IP address	<input type="checkbox"/> Indirectly from you (e.g., from observing your actions on our Services)	<input type="checkbox"/> To respond to your requests and inquiries <input type="checkbox"/> Enter into transactions with you <input type="checkbox"/> Send marketing communications	<input type="checkbox"/> Disclosure for business purposes to internet service providers
<input type="checkbox"/> Sensory data , such as Audio information from voicemail messages and/or recorded phone calls (with your consent)	<input type="checkbox"/> Directly from you	<input type="checkbox"/> To communicate with you; some phone calls are recorded (with your consent) for training our staff and for quality assurance purposes	N/A
<input type="checkbox"/> Professional or employment-related information , such as: Information regarding current occupation	<input type="checkbox"/> Directly from you	<input type="checkbox"/> To confirm eligibility for a manufacturer or lender rebate <input type="checkbox"/> To confirm eligibility for employee discount pricing	N/A
<input type="checkbox"/> Non-public education information (per the Family Educational Rights and Privacy Act (20 U.S.C. Section 1232g, 34 C.F.R. Part 99)) , such as:	<input type="checkbox"/> Directly from you	<input type="checkbox"/> To confirm eligibility for a manufacturer or lender rebate and to apply for and process any such rebate	N/A

Information regarding whether you were or would soon be a college graduate			
<input type="checkbox"/> Inferences drawn from personal information to create a profile , such as: Information regarding your vehicle preferences and needs	<input type="checkbox"/> Indirectly from you (e.g., from observing your actions on our Services) <input type="checkbox"/> Third-party service providers, including advertising companies and analytics providers	<input type="checkbox"/> To market our products and services to you	N/A

For more information regarding our privacy practices and your rights under the California Consumer Privacy Act, view our Privacy Policy at [\[insert URL for Privacy Policy\]](#).

(Rev 1/2020) Form RTK B

Template (iii): this sample form is intended for consumers who purchased/leased a vehicle, bought parts and/or obtained repair services pursuant to a parts ticket or repair order.

**RESPONSE TO REQUEST TO KNOW ABOUT CATEGORIES OF INFORMATION COLLECTED
UNDER THE CALIFORNIA CONSUMER PRIVACY ACT**

[Name of Dealership] (“Dealership,” “we,” “us” or “our”) respects the privacy of the information our customers entrust to us. This is our response to your request to know information about the following items under the California Consumer Privacy Act (CCPA):

- Categories of personal information collected;
- Categories of sources from which the personal information was collected;
- Business or commercial purposes for collecting or selling the personal information;
- Categories of third parties with whom the business shared or sold the personal information;
- Business or commercial purpose for which it sold or disclosed the personal information.

Under the CCPA, “Personal information” does not include the following items, which may be excluded from this response:

- Publicly available information, defined as information lawfully made available from federal, state, or government records;
- Protected health information;
- The sale of information to or from a consumer reporting agency for use in a consumer report;
- Personal information about a job applicant or a business’ employees (excluded from most provisions of the CCPA through December 31, 2020);
- Personal information provided in the context of a business to business communication/transaction (excluded through December 31, 2020);
- Personal information collected, processed, sold or disclosed pursuant to the Gramm-Leach-Bliley Act;
- Personal information collected, processed, sold or disclosed pursuant to the Driver’s Privacy Protection Act of 1994

Check A. or B. below

A. ☐ We are unable to confirm your identity. Your request to know about categories of personal information collected is denied.

B. ☐ The chart below reflects the information we have collected about you during the past 12 months.

Category of personal data	Source(s)	Purpose(s)	Disclosure to third parties
<input type="checkbox"/> Identifiers , such as: Name, postal address, email address, IP address, identification numbers (e.g., social security number, driver’s license number, state identification number, military identification number or passport number)	<input type="checkbox"/> Directly from you <input type="checkbox"/> Indirectly from you (e.g., from observing actions on our Services) <input type="checkbox"/> Third-party service providers, including advertising companies, analytics providers, and websites or companies that provide information regarding vehicles or	<input type="checkbox"/> To respond to your requests and inquiries <input type="checkbox"/> Communicate with you regarding our products or services <input type="checkbox"/> Enter into and process transactions with you <input type="checkbox"/> Send marketing communications <input type="checkbox"/> Complete government forms	<input type="checkbox"/> Disclosure for business purposes to internet service providers, analytics providers, payment processors and warranty, insurance or service contract administrators, if applicable to transaction <input type="checkbox"/> Disclosure for marketing purposes to advertising companies <input type="checkbox"/> Disclosure for safety and warranty purposes to vehicle

	provide listings of vehicles available for sale/lease, that forward identifiers provided by you	<input type="checkbox"/> Confirm your identity and that you are at least 18 years old <input type="checkbox"/> Confirm you are licensed to drive our vehicles or take delivery of a vehicle purchased or leased from us	manufacturer, if you purchased/leased a new or certified vehicle or if your vehicle was serviced at our dealership <input type="checkbox"/> Disclosure to state or federal agencies, when required by law <input type="checkbox"/> Disclosure to vehicle manufacturer for marketing and analytical purposes, if you purchased/leased a new or certified vehicle or if your vehicle was serviced at our dealership
<input type="checkbox"/> Personal information categories listed in the California Customer Records statute (Cal. Civ. Code § 1798.80(e)), such as: Phone number; insurance information; bank account number, credit card number, debit card number, or other financial information, including information relating to your vehicle financing or lease terms, along with vehicle information; and/or signature(s).	<input type="checkbox"/> Directly from you <input type="checkbox"/> Third-party service providers, including advertising companies and analytics providers	<input type="checkbox"/> To respond to your requests and inquiries <input type="checkbox"/> Communicate with you regarding our products or services <input type="checkbox"/> Enter into and process transactions with you <input type="checkbox"/> Send marketing communications <input type="checkbox"/> Complete government forms <input type="checkbox"/> Confirm insurance coverage <input type="checkbox"/> Confirm identity <input type="checkbox"/> Obtain authorization to collect payments <input type="checkbox"/> collect payments <input type="checkbox"/> Confirm acknowledgement of receipt of documents we provide to you	<input type="checkbox"/> Disclosure for business purposes to internet service providers, delivery services and payment processors <input type="checkbox"/> State or federal agencies, when required by law <input type="checkbox"/> Disclosure to vehicle manufacturer for marketing and analytical purposes, if you purchased/leased a new or certified vehicle or if your vehicle was serviced at our dealership
<input type="checkbox"/> Protected classification characteristics under California or federal law, such as: A photocopy/scan of government issued identification reveals personal information. For example: <ul style="list-style-type: none"> • Driver's license/state identification card - includes image, date of birth, physical description and gender • Permanent resident card - includes image, date and place of birth; • Social security card - includes social security number 	<input type="checkbox"/> Directly from you <input type="checkbox"/> Government's Military Lending Act website	<input type="checkbox"/> To confirm identity <input type="checkbox"/> Confirm you are licensed to drive our vehicles or take delivery of a vehicle purchased or leased from us <input type="checkbox"/> Confirm eligibility for a manufacturer or lender rebate and to apply for and process any such rebate <input type="checkbox"/> Determine coverage under the Military Lending Act in connection with a financed vehicle transaction <input type="checkbox"/> Provide you with copies of certain documents written in the language in which your finance or lease transaction was primarily negotiated, as required by law	<input type="checkbox"/> Disclosure to manufacturer or lender for processing applicable rebate <input type="checkbox"/> Disclosure to state or federal agencies, when required by law

<ul style="list-style-type: none"> • Passport - includes image, date and place of birth and nationality • Military ID - includes image and rank <p>Completion of a Translated Contract Acknowledgement or signing of translated documents reveals your primary language</p>		<input type="checkbox"/> Complete government forms	
<input type="checkbox"/> Commercial information , such as: Vehicle information, ownership information, and current lease or finance terms	<input type="checkbox"/> Directly from you <input type="checkbox"/> Third parties, such as vehicle manufacturer and/or advertising companies	<input type="checkbox"/> Enter into and process transactions with you <input type="checkbox"/> Appraise your vehicle <input type="checkbox"/> Send informational and marketing communications <input type="checkbox"/> Retain records of transactions as required by law <input type="checkbox"/> Fulfill the terms of a written warranty or product recall <input type="checkbox"/> Process warranty, insurance or service contract claims <input type="checkbox"/> Share information with state agencies as required by law	<input type="checkbox"/> Disclosure for business purposes to payment processors, delivery services and warranty, insurance or service contract administrators, if applicable to transaction <input type="checkbox"/> Disclosure for safety and warranty purposes to vehicle manufacturer, if you purchased/leased a new or certified vehicle or if your vehicle was serviced at our dealership <input type="checkbox"/> Disclosure to state or federal agencies, when required by law
<input type="checkbox"/> Biometric information You completed a "Thumbprint form"	<input type="checkbox"/> Directly from you	<input type="checkbox"/> To confirm identity	N/A
<input type="checkbox"/> Internet or other similar network activity information , such as: IP address, browsing history, and search history	<input type="checkbox"/> Indirectly from you (e.g., from observing your actions on our Services)	<input type="checkbox"/> To communicate with you regarding our products and services <input type="checkbox"/> Improve user experiences by making our website easier to use and navigate, and more personalized based on the profile we create about you	<input type="checkbox"/> Disclosure for business purposes to internet service providers
Geolocation information , such as: <input type="checkbox"/> IP address <input type="checkbox"/> Vehicle location (using GPS, as permitted by law)	<input type="checkbox"/> Indirectly from you (e.g., from observing your actions on our Services) <input type="checkbox"/> From vehicles equipped with GPS tracking (as permitted by law)	<input type="checkbox"/> To respond to your requests and inquiries <input type="checkbox"/> Enter into and process your transactions with you <input type="checkbox"/> Send marketing communications <input type="checkbox"/> Track vehicles as permitted by law	<input type="checkbox"/> Disclosure for business purposes to internet service providers
<input type="checkbox"/> Sensory data , such as	<input type="checkbox"/> Directly from you	<input type="checkbox"/> To communicate with you; some phone calls are recorded (with your consent) for	N/A

Audio information from voicemail messages and/or recorded phone calls (with your consent)		training our staff and for quality assurance purposes	
<input type="checkbox"/> Professional or employment-related information , such as: Information regarding current occupation	<input type="checkbox"/> Directly from you	<input type="checkbox"/> To confirm eligibility for a manufacturer or lender rebate and to apply for and process any such rebate, if applicable <input type="checkbox"/> To confirm eligibility for employee discount pricing <input type="checkbox"/> Complete government forms, as required	<input type="checkbox"/> Disclosure to manufacturer or lender for processing rebate, if applicable <input type="checkbox"/> Disclosure to state or federal agencies, when required by law
<input type="checkbox"/> Non-public education information (per the Family Educational Rights and Privacy Act (20 U.S.C. Section 1232g, 34 C.F.R. Part 99)) , such as: Information regarding whether you were or would soon be a college graduate	<input type="checkbox"/> Directly from you	<input type="checkbox"/> To confirm eligibility for a manufacturer or lender rebate and to apply for and process any such rebate, if applicable	<input type="checkbox"/> Disclosure to manufacturer or lender for processing rebate, if applicable
<input type="checkbox"/> Inferences drawn from personal information to create a profile , such as: Information regarding your vehicle preferences and needs	<input type="checkbox"/> Indirectly from you (e.g., from observing your actions on our Services) <input type="checkbox"/> Third-party service providers, including advertising companies and analytics providers	<input type="checkbox"/> To market our products and services to you	N/A

For more information regarding our privacy practices and your rights under the California Consumer Privacy Act, view our Privacy Policy at [\[insert URL for Privacy Policy\]](#).

(Rev 1/2020) Form RTK C

*This sample response is for responding to a consumer who requests to know the **specific pieces** of personal information that have been collected. Before providing this sensitive information, dealers should review page 34 of this Handbook regarding Verification of Requests.*

**RESPONSE TO REQUEST TO KNOW ABOUT SPECIFIC PIECES OF PERSONAL INFORMATION
UNDER THE CALIFORNIA CONSUMER PRIVACY ACT**

To: [Name of Requester]

Date of receipt of request: _____

Date of response to request: _____

[Name of Dealership] ("Dealership," "we," "us" or "our") respects the privacy of the information our customers entrust to us. This is our response to your request to know the specific pieces of information collected about you, under the California Consumer Privacy Act.

- ☐ We are unable to locate in our records any personal information relating to you.
- ☐ We are unable to confirm your identity. Your request to know the specific pieces of personal information is denied.
- ☐ In the past 12 months, we collected the following specific pieces of information about you:

Name: _____
 Phone number(s): _____
 Email address: _____
 Mailing address: _____
 IP address: _____
 Other: _____
 Other: _____

- ☐ For customers who have purchased or leased a vehicle from the Dealership, have purchased parts, or have had their vehicles serviced at the Dealership pursuant to a parts ticket or repair order, enclosed with this response is a redacted* copy of documents containing specific pieces of personal information collected from you.

For more information regarding our privacy practices and your rights under the California Consumer Privacy Act, view our Privacy Policy at [\[insert URL for Privacy Policy\]](#).

*For your privacy, we have not identified and have redacted from the enclosed documents the following pieces of personal information collected from you: social security number, driver's license number or other government-issued identification number, financial account number, any account password, or security questions and answers.

(Rev 1/2020) Form RTKSP

I. Sample Data Retention Policy

Please note the record retention policy mentioned below may be the record retention policy available through CNCDA or a dealership-specific record retention policy.

DATA RETENTION POLICY

Purpose

The purpose of this Data Retention Policy (“Policy”) is to ensure that the data collected, maintained and used by DEALERSHIP (“DEALERSHIP”), including sensitive personal data, is adequately protected and maintained, and to ensure that data that is no longer needed by DEALERSHIP is discarded at the proper time and in the proper manner. This Policy is designed to ensure compliance with U.S. federal and local laws and regulations to eliminate accidental or innocent destruction of documents, and to facilitate DEALERSHIP’s operations by promoting efficiency and freeing up valuable storage space. This Policy is also for the purpose of aiding employees of DEALERSHIP in understanding their obligations in retaining information. DEALERSHIP expects all employees to fully comply with this Policy.

Definitions of Key Terms

“**Data**” is defined as any written, recorded or graphic material of any kind existing in any tangible or electronic form that is in the custody, possession or control of DEALERSHIP or any of its directors, officers or employees, which in any way concerns DEALERSHIP’s operations, business activities or legal requirements, including, but not limited to customer personal data. Data may be as obvious as a memorandum, an email, a contract, or something not as obvious, such as a computerized desk calendar, an appointment book, or an expense record.

“**Retention Period**” is defined as the period of time during which Data must be retained. Unless otherwise specified, Retention Periods are measured from the date of Data creation or modification.

Requirements

All Data will be stored in the physical locations or in the electronic systems that DEALERSHIP has provided and designated for such Data. Data shall be retained in a manner that reasonably protects the Data from damage or destruction, facilitates the location and retrieval of the Data in a minimal amount of time and with minimal expense and effort, and complies with other DEALERSHIP policies and procedures, to the extent applicable. Following the expiration of the Retention Period, Data should be destroyed absent explicit written direction to the contrary from [INSERT PERSON IN CHARGE OF ENFORCING THIS POLICY].

Before Data is disposed of or destroyed, DEALERSHIP must verify that the Data (i) has met its Retention Period and (ii) is not the subject of any pending/imminent/threatened litigation or audit (see Section VI below for more information about this exception). Data will be disposed of in a manner that is reasonable considering the content of the Data, but which assures that the information has been destroyed.

- For printed Data:
 - Confidential or sensitive Data should be shredded or incinerated.
 - All non-confidential Data may be disposed of in the appropriate recycling receptacle.
- For electronic Data:
 - All Data should be deleted in a way that is irretrievable and non-restorable.

Email Archival Practices

This section is designed to ensure compliance with federal and state laws and regulations, to eliminate accidental or innocent destruction of emails and to facilitate DEALERSHIP's operations by promoting efficiency and freeing up valuable storage space. This section sets general guidelines, recognizing the impracticality of adhering to rigid rules, and the massive volume of records created by the ever-growing collection of digital devices and services used within DEALERSHIP.

DEALERSHIP strives to keep emails as follows:

- Retention settings are set to generally "archive" any messages over 6 months of age. These retained messages will be removed from the mail server to reduce the need for storage space.
- The messages will then be archived for up to 7 years, unless a longer or shorter Retention Period is chosen for selected messages.
- Retention settings should apply to all general mail storage folders including inbox and sent messages.
- If an employee uses electronic messages for business, outside a corporate email system account, the employee is expected to make reasonable effort to make records of the messages such that they are within DEALERSHIP's control.

Litigation Exception Process and How to Respond to Discovery Requests

In the event that DEALERSHIP is served with any subpoena or request for Data or any employee becomes aware of a governmental investigation or audit concerning DEALERSHIP or the commencement of any litigation against or concerning DEALERSHIP, such employee shall inform [INSERT PERSON IN CHARGE OF ENFORCING THIS POLICY] and any further disposal of Data shall be suspended until such time as [INSERT PERSON IN CHARGE OF ENFORCING THIS POLICY], with the advice of legal counsel, determines otherwise. [INSERT PERSON IN CHARGE OF ENFORCING THIS POLICY] shall take such steps as are necessary to promptly inform all employees of any suspension in the further disposal of Data. This exception supersedes any previously or

subsequently established destruction schedule for those Data. If you believe this exception may apply, or have any questions regarding the possible applicability of this exception, or if you believe, for any reason, that Data or category of Data should not be destroyed, please contact [INSERT PERSON IN CHARGE OF ENFORCING THIS POLICY].

Data Retention Schedule

It is impossible to designate a Retention Period for each and every type of Data that may exist or come to exist. However, this Policy sets forth Retention Periods for certain common types of Data in the chart below. If certain Data does not fall within a class for which there is a designated Retention Period in this Policy, DEALERSHIP will consult with legal counsel to determine the proper classification of the Data or to establish a Retention Period for the Data in question. To the extent Data is subject to more than one Retention Period, the Data will be retained for the longer of the specified time frames in order to comply with this Policy.

[INSERT RECORD RETENTION SCHEDULE]

J. CIS Critical Security Controls for Effective Cyber Defense Checklist

The Center for Internet Security (CIS) Controls are a set of security best practices that are used by organizations around the world. In 2016, the California Attorney General cited to the CIS Controls as a reference to reasonable security in the office's 2016 Data Breach Report. This checklist may be used as a means of determining whether the dealership and its vendors have reasonable security measures in place.

		YES	NO
1.	Inventory of Authorized and Unauthorized Devices		
		YES	NO
2.	Inventory of Authorized and Unauthorized Software		
		YES	NO
3.	Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers		
		YES	NO
4.	Continuous Vulnerability Assessment and Remediation		
		YES	NO
5.	Controlled Use of Administrative Privileges		
		YES	NO
6.	Maintenance, Monitoring, and Analysis of Audit Logs		
		YES	NO
7.	Email and Web Browser Protections		
		YES	NO
8.	Malware Defenses		
		YES	NO
9.	Limitation and Control of Network Ports, Protocols, and Services		
		YES	NO
10.	Data Recovery Capability		
		YES	NO
11.	Secure Configurations for Network Devices such as Firewalls, Routers, and Switches		
		YES	NO
12.	Boundary Defense		
		YES	NO
13.	Data Protection		
		YES	NO
14.	Controlled Access Based on the Need to Know		
		YES	NO
15.	Wireless Access Control		
		YES	NO
16.	Account Monitoring and Control		

		YES	NO
17.	Security Skills Assessment and Appropriate Training to Fill Gaps		
		YES	NO
18.	Application Software Security		
		YES	NO
19.	Incident Response and Management		
		YES	NO
20.	Penetration Tests and Red Team Exercises		

K. Sample Data Processing Agreement**DATA PROCESSING ADDENDUM**

This Data Processing Addendum (“DPA”) forms part of the Agreement (“Principal Agreement”) between (i) _____ (“VENDOR”) and (ii) _____ (“DEALERSHIP”) dated _____.

1. DEFINITIONS

1.1 **“Data Subject”** means a living individual who is the subject of any of the Personal Data;

1.2 **“Data Privacy Legislation”** means all laws and regulations, in any country of the world, which protect the privacy rights of individuals, in so far as those laws and regulations apply to the Processing of Personal Data in connection with this DPA;

1.3 **“Personal Data Security Breach”** means any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, access to, acquisition of, or use of any Personal Data;

1.4 **“Personal Data”** shall mean any information that VENDOR has received or collected for processing pursuant to the Principal Agreement that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, to a particular consumer or household;

1.5 **“Processing”** shall mean any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure, or destruction.

2. OWNERSHIP

Each party hereby acknowledges and agrees that DEALERSHIP owns all rights, title, and interest in and to the Personal Data which is processed by VENDOR on behalf of DEALERSHIP pursuant to the Principal Agreement.

3. DATA PRIVACY

VENDOR must:

3.1 Comply with Data Privacy Legislation, and use all reasonable endeavors to assist DEALERSHIP in its own compliance with Data Privacy Legislation, in connection with this DPA;

3.2 Not do, or cause or permit to be done, anything in relation to the information provided to or processed by VENDOR which may result in a breach by DEALERSHIP of any applicable laws, regulations, regulatory requirements, or the Data Privacy Legislation;

3.3 Only process the Personal Data in accordance with DEALERSHIP's documented instructions, which may be specific instructions or standing instructions of general application in relation to the performance of VENDOR's obligations under this DPA, unless otherwise required by law. In particular, VENDOR shall not: (i) sell the Personal Data or share the Personal Data with any third parties without DEALERSHIP's permission; (ii) retain, use or disclose the Personal Data for any purpose other than the purposes specified in the Principal Agreement, including retaining, using or disclosing the Personal Data for a commercial purpose other than to provide VENDOR's services to DEALERSHIP; and (iii) retain, use or disclose the Personal Data outside of VENDOR's business relationship with DEALERSHIP;

3.4 Put in place measures to ensure that any employees who have access to Personal Data: (i) do not process the data except on instructions from DEALERSHIP, unless required to do so by law; (ii) are subject to confidentiality undertakings or professional or statutory obligations of confidentiality; and (iii) comply with applicable Data Privacy Legislation in the context of that individual's duties to DEALERSHIP;

3.5 Not disclose the Personal Data to any other body (including any subprocessor) without DEALERSHIP's express agreement in writing;

3.6 Not subcontract to a subprocessor any of VENDOR's duties under this DPA unless: (i) VENDOR has obtained prior express agreement in writing from DEALERSHIP; and (ii) the subprocessor is subject to a written agreement which imposes on the subprocessor the same obligations that are imposed on you under this DPA. Any consent which DEALERSHIP gives pursuant to this clause or this DPA generally for subcontracting will not relieve VENDOR from any liability for the performance of its obligations under this DPA;

3.7 Comply with all reasonable requests or directions by DEALERSHIP to enable it to verify and/or procure that VENDOR is in full compliance with its obligations under this DPA;

3.8 Upon termination of its provision of services, delete or return all Personal Data to DEALERSHIP and delete any existing copies of the Personal Data, save where applicable law requires VENDOR to retain copies of such data. VENDOR shall provide written certification that it and each of its subprocessors have fully complied with this section within 60 days of the termination of the provision of services.

4. SECURITY

VENDOR must:

4.1 At a minimum, implement and maintain reasonable technical and organizational measures to ensure the security and protection of Personal Data, taking into account the nature and sensitivity of the information to be protected, the risk presented by Processing, the state of the art, and the costs of implementation, in compliance with applicable Data Privacy Legislation;

4.2 Immediately notify DEALERSHIP if VENDOR knows, discovers or reasonably believes that there has been any Personal Data Security Breach;

4.3 In the event of a Personal Data Security Breach, (i) immediately investigate, correct, mitigate, remediate and otherwise handle the Personal Data Security Breach, including without limitation, by identifying Personal Data affected by the Personal Data Security Breach and taking sufficient steps to prevent the continuation and recurrence of the Personal Data Security Breach; and (ii) provide information and assistance needed to enable DEALERSHIP to evaluate the Personal Data Security Breach and, as applicable, to comply with any obligations to provide timely notice to affected individuals or information about the Personal Data Security Breach to relevant regulators; and

4.4 Reimburse DEALERSHIP for the reasonable expenses that DEALERSHIP may incur as a result of such Personal Data Breach caused by VENDOR's acts or omissions or those of any of VENDOR's authorized subprocessors, including but not limited to, the expenses incurred in investigating the Personal Data Security Breach and notifying affected individuals, and providing these individuals with the support necessary under the circumstances, such as credit monitoring.

5. LIABILITY AND INSURANCE

Notwithstanding anything to the contrary in the Principal Agreement, VENDOR's total aggregate liability, including any liability for subprocessors, under or in connection with this DPA, shall not exceed \$_____. VENDOR presently maintains and will continue to maintain in force, at VENDOR's sole expense, the following insurance: Cyber Risk and Privacy Liability Insurance Policy, or similar policy with a nationally recognized insurance company licensed to do business in California and DEALERSHIP as a named insured having a minimum limitation of liability of \$_____.

6. INDEMNITY

VENDOR will indemnify and hold harmless DEALERSHIP and its officers, directors and employees from and against all third-party claims and legal actions brought against DEALERSHIP arising out of VENDOR's breach or alleged breach of this DPA, or in the event of any injury to any person, damage to or loss of property, or any other claim arising out of or resulting from any act or omission of VENDOR, its employees, agents or subprocessors in connection with or arising out of the performance of this DPA, including without limit, any losses, liabilities, damages, judgments, fines, penalties, costs or expenses, including court costs and reasonable legal and investigation costs awarded against or incurred by DEALERSHIP. DEALERSHIP shall have the right, at its cost, to participate in the defense of any claims concerning matters that relate to DEALERSHIP. VENDOR

may not enter into any settlement without DEALERSHIP's express written consent (which shall not be unreasonably withheld), unless such settlement (i) releases DEALERSHIP in full for all claims, (ii) does not impose any obligation on DEALERSHIP, other than amounts to be paid directly by VENDOR (and not DEALERSHIP), and (iii) includes no admission of any kind by or on behalf of DEALERSHIP.

7. CONSUMER REQUESTS UNDER THE CALIFORNIA CONSUMER PRIVACY ACT (CCPA)

If DEALERSHIP provides written notification to VENDOR of a consumer's request to delete his or her Personal Data, within ten (10) business days of the date the request is sent, VENDOR shall delete all such information from VENDOR's records and provide written confirmation to DEALERSHIP that the information has been deleted. CCPA deletion requests shall be sent by email to VENDOR at the following email address [INSERT EMAIL ADDRESS] or by U.S. mail to VENDOR's address at [INSERT POSTAL ADDRESS]. If a consumer whose information is subject to this Agreement makes a deletion request or other data subject request directly to VENDOR, VENDOR shall notify DEALERSHIP at the following email address [INSERT EMAIL ADDRESS] or by U.S. mail to DEALERSHIP's address at [INSERT POSTAL ADDRESS]. DEALERSHIP will provide VENDOR with instructions for handling the request in compliance with the CCPA and VENDOR agrees to act in accordance with DEALERSHIP's instructions.

IN WITNESS WHEREOF, this Data Processing Addendum is entered into and becomes a binding part of the Principal Agreement with effect from [INSERT DATE].

DEALERSHIP

Signature _____

Name _____

Title _____

Date Signed _____

VENDOR

Signature _____

Name _____

Title _____

Date Signed _____

L. Short Form Service Provider Agreement Regarding Compliance With CCPA**ADDENDUM REGARDING COMPLIANCE WITH CALIFORNIA CONSUMER PRIVACY ACT**

This Addendum forms part of the Agreement (“Principal Agreement”) between (i) _____ (“Service Provider”) and (ii) _____ (“Dealership”) dated _____.

For purposes of this Addendum, “Personal Data” shall mean any information that Service Provider has received or collected for processing pursuant to the Principal Agreement that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, to a particular consumer or household.

Service Provider agrees to maintain physical, electronic and procedural safeguards that comply with state and federal laws in order to protect the confidentiality of all Personal Data regarding Dealership’s customers.

Service Provider is prohibited from:

- (a) selling the Personal Data;
- (b) retaining, using, or disclosing the Personal Data for any purpose other than for the specific purpose of performing the services specified in the Principal Agreement, including retaining, using, or disclosing the Personal Data for a commercial purpose other than providing the services specified in the Principal Agreement;
- (c) further collecting, selling, or using the Personal Data except as necessary to perform the business purpose specified in the Principal Agreement; and
- (d) retaining, using, or disclosing the information outside of the direct business relationship between Service Provider and Dealership.

The undersigned certifies that Service Provider understands and restrictions set forth above and will comply with each of them.

Service Provider

Signature _____

Name _____

Title _____

Date Signed _____

M. Sample Incident Response Manual

INCIDENT AND BREACH RESPONSE PLAN

Overview

- I. Definitions**
- II. The Team**
- III. Reporting an Incident**
- IV. The First 24 Hours**
- V. Notifying Law Enforcement**
- VI. Next Steps**
- VII. Notifying Data Breach Victims**
- VIII. Managing Communications**
- IX. Review Response and Update Policies**
- X. Auditing Your Plan**
- XI. Template Breach Notification Letter**
- XII. NIST Checklist**

I. DEFINITIONS

“Breach” or “Data Breach” means an incident resulting in the unlawful and unauthorized access or acquisition of personal information that compromises the security, confidentiality, and integrity of that personal information.

“Event” means any observable occurrence in a system or network, such as a server receiving a request for a web page, a user sending an email message, or a firewall blocking an attempt to make a connection.

“Incident” means an event that violates an organization’s security policies and procedures.

“Personal Information,” is not universally defined in the U.S. In California, it means an individual’s first name or first initial and last name, plus one or more of the following: SSN, driver’s license, state ID, account number, credit card or debit card number combined with the security code, PIN, or password needed to access an account. State breach notification laws vary on the definition of personal information and legal counsel should be consulted regarding the precise definitions that may apply. Multiple state laws may apply to one data breach because jurisdiction depends on where the affected individuals reside.

II. THE TEAM

Assembling a complete team (Incident Response Team) comprised of strong, capable representatives will go a long way toward ensuring an efficiently executed response. Your Incident Response Team should include the following constituents, as applicable:

❖ **Incident Lead**

- Determines when the full Incident Response Team needs to be activated in response to an incident;
- Manages and coordinates DEALERSHIP's overall response efforts and team, including establishing clear ownership of priority tasks;
- Acts as an intermediary between execs and other team members to report on progress and problems;
- Ensures proper documentation of incident response process and procedures.

❖ **Information Technology and Security**

- Identifies top security risks that should be incorporated into written incident response plans;
- Trains personnel in data breach response, including securing the premises, safely taking infected machines offline, and preserving evidence;
- Works with forensics to identify the compromised data and deletes hacker tools without compromising evidence and progress.

❖ **Legal and Privacy**

- Determines how to notify affected individuals, the media, law enforcement, government agencies and other third parties;
- Establishes relationships with any necessary external legal counsel before a breach occurs;
- Final sign-off on all written materials related to the incident.

❖ **Law Enforcement (depending on the severity of the breach)**

- Looks for evidence that a crime has been committed.

❖ **Forensics**

- Advise DEALERSHIP on how to stop data loss, secure evidence, and prevent further harm;
- Preserve evidence and manage the chain of custody, minimizing the chance that evidence will be altered, destroyed, or rendered inadmissible in court.

III. REPORTING AN INCIDENT

Regardless of origin, all information security events, incidents and breaches must be funneled through IT, which can be contacted at [INSERT CONTACT INFORMATION]. It is the central point of contact before the Incident Response Team is engaged.

IV. THE FIRST 24 HOURS

Acting swiftly and strategically following a security incident can help you regain your security, preserve evidence, and protect your brand. Always collect, document and record as much information about the incident and your response efforts as possible, including conversations with law enforcement and legal counsel.

1. **Record the moment of discovery** – Also mark the date and time your response efforts begin, i.e. when someone on the Incident Response Team is alerted to the incident.
2. **Alert and activate everyone** – Include everyone on the Incident Response Team, including external resources, to begin executing your preparedness plan.
3. **Analyze** – The Incident Response Team will review the nature of the incident, including whether the incident is a breach, and the severity of the incident.
4. **Secure the premises** – Ensure the area where the incident occurred and surrounding areas are secure to help preserve evidence.
5. **Stop additional data loss** – Take affected machines offline, but do not turn them off or start probing into the computer until the forensics team arrives.
6. **Document everything** – Record who discovered the incident, who reported it, to whom it was reported, who else knows about it, what type of incident it was (i.e. phishing attack, malware attack), etc.
7. **Interview involved parties** – Speak with those involved with discovering the incident and anyone else who may know about it—then document the results.
8. **Review notification protocols** – Review those that touch on disseminating information about the incident for everyone involved in this early stage.
9. **Assess priorities and risks** – Include those based on what you know about the incident. If required, bring in a forensics firm to begin an in-depth investigation.
10. **Bring in a forensics firm** – Begin an in-depth investigation.
11. **Notify law enforcement** – Do this if needed, after consulting with legal counsel and upper management.

V. NOTIFYING LAW ENFORCEMENT

If there is reasonable evidence of a crime, rather than simply an event or occurrence that resulted in a security incident, you should notify law enforcement. A preliminary inquiry should include:

- Ruling out normal hardware or software failure.
- Developing a chronology of what happened.
- Auditing for any unusual activity during that time frame.
- Identifying any users or processes involved.
- Evaluating the motives of any actors.

VI. NEXT STEPS

After the first day, assess your progress to ensure your plan is on track. Then, continue with these steps:

1. **Identify the root cause** – Ensure your forensics team removes hacker tools, and address any other security gaps. Document when and how the incident was contained.
2. **Alert your external partners** – If there was a breach, notify your partners, including your insurance carrier, and include them in the incident response moving forward. If required, engage a data breach resolution vendor to handle notifications and set up a call center.
3. **Continue working with forensics** – Determine if any countermeasures, such as encryption, were enabled during the incident. Analyze all data sources to ascertain what information was compromised.
4. **Identify legal obligations** – Revisit state and federal regulations that apply and then determine all entities that need to be notified. Ensure all notifications occur within any mandated timeframes.
5. **Report to upper management** – Generate reports that include all the facts about the incident, as well as the steps and resources needed to resolve it. Create a high-level overview of priorities and progress, as well as problems and risks.
6. **Identify conflicting initiatives** – Determine if any upcoming business initiatives may interfere or clash with response efforts. Decide whether to postpone these efforts and for how long.
7. **Evaluate response and educate employees** – Once an incident is resolved, evaluate how effectively your company managed its response in order to make the necessary improvements to your preparedness plan. Taking time to reflect and make these adjustments will ensure a smoother response in the future. Use the incident as an opportunity to retrain employees not only in their specific response role when a security incident occurs, but also in their own security and privacy practices.

VII. NOTIFYING DATA BREACH VICTIMS

Not all breaches require a notification. When they do, it is your responsibility to determine the deadlines for notification according to state law. **Multiple state laws may apply to one data breach because jurisdiction depends on where the affected individuals reside, not where the business is located or where the breach occurred.** Typically, businesses have 60 days to notify affected individuals of a data breach when notification is required by law. Certain state laws and federal regulations shrink the timeline to 30 or 45 days. The countdown starts the moment a

breach is discovered. Notification may be delayed if law enforcement believes it would interfere with an ongoing investigation.

California law requires a business or state agency to notify any California resident whose unencrypted personal information was acquired, or reasonably believed to have been acquired, by an unauthorized person. California's data breach notification statute⁶⁴ defines personal information as first name or first initial and last name, **plus**: Social Security number; driver's license or state identification card number; financial account, credit or debit card number, in combination with any required security or access code or password permitting access to a resident's financial account; medical or health insurance info; or info collected by automated license plate recognition systems. It also includes a username or email address, in combination with a password or security question and answer that would permit access to an online account. The statute does not apply to encrypted information so long as the encryption key was not or is not reasonably believed to have been acquired. Notification must 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 of the system.

Some states mandate specific content for you to include in your notification letters. This can include toll-free numbers and addresses for the three major credit bureaus, the Federal Trade Commission and a state's attorney general. As dictated by state law, a notification letter should include:

- Clear language, not industry jargon, that the average person could understand.
- A toll-free phone number for individuals wanting additional information.
- Details about the type of data lost and how it was lost, unless prohibited by law.
- Next steps to help affected individuals regain their security, such as signing up for a complimentary identity protection product.

Under California law, notice must be in "plain language," use at least 10-point font, and organized by clearly and conspicuously displayed titles and headings. Notice must include the name and contact info of the covered entity; the types of covered info that were the subject of the breach; the date, estimated date, or date range of the breach; the date of the notice; whether notice was delayed due to law enforcement; general description of the breach; and toll-free numbers and addresses of the major credit reporting agencies, if Social Security numbers, drivers' license or state identification card numbers were exposed. If Social Security, drivers' license or state identification card numbers are affected, and if the entity providing notice was the source of the breach, the entity must offer appropriate identity theft prevention and mitigation services, such as credit monitoring, at no cost to the resident for not less than 12 months. A template notification letter for California is provided in Section XIII.

⁶⁴ Civil Code Section 1798.82.

Mishandling notifications can lead to severe consequences, including fines and other unbudgeted expenses. It could also tarnish your brand reputation and customer loyalty, leading to potential revenue loss.

VIII. MANAGING COMMUNICATIONS

You should develop a communications incident response process and plan that clearly outlines who will be responsible for developing and approving the key messages that will be communicated to media, as well as internal audiences. Communicating the right messages at the proper points in the lifecycle of a breach will have a significant impact on how a breach is reported.

- Focus initial messages on the steps being taken to investigate the issue and frame it as a criminal issue.
- Think through what you push out and how to respond via social channels. There's no need to have a public debate in front of millions of followers.
- Set up the appropriate media/social monitoring and listening posts to see how the breach is being covered.
- Customers must be your north star, so make sure that you communicate with them clearly and effectively through traditional and digital channels.
- Do not neglect the wide variety of stakeholders interested in breaches, including policymakers, regulators (state and federal), and industry stakeholders (e.g. payment brands).

IX. REVIEW RESPONSE AND UPDATE POLICIES

In the aftermath of a security incident, you must plan and take preventative steps so a similar incident cannot happen again. Consider whether:

- An additional policy could have prevented the incident.
- A procedure or policy was not followed which allowed for the incident, and then consider what could be changed to ensure that the procedure or policy is followed in the future.
- Any security policies need to be updated.
- Any lessons can be learned from this experience. The longer you wait to document lessons learned, the less likely it is that the lessons learned will be documented accurately and completely.

X. AUDITING THE PLAN

Auditing your preparedness plan helps ensure it stays current and useful. The chart below will help you audit your plan.

Status	Action	Timing
	Update data breach Incident Response Team contact list. <ul style="list-style-type: none"> • Check that contact information for internal and external members of your breach Incident Response Team is current. • Remove anyone who is no longer with your company or with an external partner and add new department heads. • Redistribute the updated list to the appropriate parties. 	Quarterly
	Verify your data breach response plan is comprehensive. <ul style="list-style-type: none"> • Update your plan, as needed, to take into account any major company changes, such as recently established lines of business, departments or data management policies. • Verify that each Incident Response Team member and department understands its role during a data breach. Create example scenarios for your Incident Response Team and departments to address. 	Quarterly
	Double check your vendor contracts. <ul style="list-style-type: none"> • Ensure you have valid contracts on file with your forensics firm, data breach resolution provider and other vendors. • Verify that your vendors and contracts still match the scope of your business. 	Quarterly
	Review notification guidelines. <ul style="list-style-type: none"> • Ensure the notification portion of your response plan takes into account the latest state legislation. • Update your notification letter templates, if any, as needed, to reflect any new laws. • Verify your contacts are up to date for the attorneys, government agencies or media you will need to notify following a breach. 	Quarterly
	Check up on third parties that have access to your data. <ul style="list-style-type: none"> • Review how third parties are managing your data and if they are meeting your data protection standards. This is done during the due diligence process. • Ensure they are up to date on any new legislation that may affect you during a data breach. • Verify they understand the importance of notifying you immediately of a breach and working with you to resolve 	Quarterly

	it. This should be addressed in your contract with the vendor.	
	Evaluate IT Security. <ul style="list-style-type: none"> • Ensure proper data access controls are in place. • Verify that company-wide automation of operating system and software updates are installing properly. • Ensure automated monitoring of and reporting on systems for security gaps is up to date. • Verify that backup tapes are stored securely. 	Quarterly
	Review staff security awareness. <ul style="list-style-type: none"> • Ensure everyone on staff is up to date on proper data protection procedures, including what data, documents and emails to keep and what to securely discard. • Review how to spot and report the sign of a data breach from within everyday working environments. • Verify that employees are actively keeping mobile devices and laptops secure onsite and offsite and changing passwords every three months. 	Yearly

XI. TEMPLATE CALIFORNIA BREACH NOTIFICATION LETTER

All breach notification letters should be reviewed by legal counsel before being sent out.

[NAME OF DEALERSHIP/LOGO]	
Date: [INSERT]	
NOTICE OF DATA BREACH	
What Happened?	[INSERT DESCRIPTION OF THE INCIDENT]
What Information Was Involved?	[INSERT DESCRIPTION OF INFORMATION INVOLVED]
What We Are Doing.	[INSERT DESCRIPTION OF WHAT DEALERSHIP IS DOING TO MITIGATE THE INCIDENT]
What You Can Do.	<p>We recommend the following steps that you can take to protect your information:</p> <ul style="list-style-type: none"> • Credit Report Monitoring [INSERT IF YOU ARE OFFERING CREDIT MONITORING] • Monitor Your Credit Reports Even if you choose not to take advantage of this complimentary credit monitoring service, we remind you to remain vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every

12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

Experian, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft, as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft.

- **Fraud Alert**

There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

	<ul style="list-style-type: none"> • Fair Credit Reporting Act You also have rights under the federal Fair Credit Reporting Act, which promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. The FTC has published a list of the primary rights created by the FCRA (https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf), and that article refers individuals seeking more information to visit www.ftc.gov/credit. The FTC's FCRA rights include: <ul style="list-style-type: none"> – You have the right to receive a copy of your credit report. The copy of your report must contain all the information in your file at the time of your request. – Each of the nationwide credit reporting companies – Experian, TransUnion and Equifax – is required to provide you with a free copy of your credit report, at your request, once every 12 months. – You are also entitled to a free report if a company takes adverse action against you, like denying your application for credit, insurance, or employment, and you ask for your report within 60 days of receiving notice of the action. The notice will give you the name, address, and phone number of the credit reporting company. You're also entitled to one free report a year if you're unemployed and plan to look for a job within 60 days; if you're on welfare; or if your report is inaccurate because of fraud, including identity theft. – You have the right to ask for a credit score. – You have the right to dispute incomplete or inaccurate information. – Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information. – Consumer reporting agencies may not report outdated negative information. – Access to your file is limited. And you must give your consent for reports to be provided to employers. – You may limit "prescreened" offers of credit and insurance you get based on information in your credit report. – You may seek damages from violators. – Identity theft victims and active duty military personnel have additional rights.
Other Important Information.	You may wish to review the tips provided by the Federal Trade Commission on how to avoid identity theft. For more information, please visit www.ftc.gov/idtheft or call 1-877-438-4338.

For More Information.	Call [TELEPHONE NUMBER] or go to [WEBSITE].
------------------------------	---

XII. NIST CHECKLIST OF ELEMENTS INCLUDED IN A RECOVERY PLAYBOOK

In addition, the National Institute of Standards and Technology (NIST) provides the following checklist of elements to be included in a recovery playbook:

A.1 Pre-Conditions Required for Effective Recovery

The organization understood the need to be prepared and conducted planning to operate in a diminished condition. The playbook includes the following critical elements:

- A set of formal recovery processes.
- The criticality of organizational resources (e.g., people, facilities, technical components, external services) that are required to achieve the organization’s mission(s).
- Functional and security dependency maps to understand the order of restoration priority.
- A list of technology and personnel who will be responsible for defining and implementing recovery criteria and associated plans.
- A comprehensive recovery communications plan with fully integrated internal and external communications considerations, including information sharing criteria informed by recommendations in NIST SP 800-150 [11].

A.2 Tactical Recovery Phase

The following steps summarize the activities of the recovery team in the tactical recovery phase.

A.2.1 Initiation

- Receive a briefing from the incident response team to understand the extent of the cyber event.
- Determine the criticality and impact of the cyber event.
- Formulate an approach and set of specific actions.
- Heighten monitoring and alerting of the network and systems.
- Understand the adversary’s motivation.
- Identify the adversary’s footprint on the infrastructure, command and control channels, and tools and techniques.
- Inform all parties that the recovery activities have been initiated.
- Utilize all available information gathered to create the restoration plan.

A.2.2 Execution

- Begin to execute the restoration by validating and implementing remediation countermeasures in coordination with the incident response team and other information security personnel.
- Restore additional business services and communicate the restoration status with predefined parties.
- Track the actual time that critical services were unavailable or diminished, comparing the actual outage with agreed-upon service levels and recovery times.
- Document any issues that arise, any indicators of compromise, and newly identified dependencies.
- Coordinate with representatives from management, senior leadership, HR and legal to discuss appropriate notification activities.
- Additional recovery steps are initialized, including external interactions and services to restore confidence and to protect constituents.
- Validate that the restored assets are fully functional and meet the security posture required by the security team.

A.2.3 Termination

- Determine that termination criteria have been met and declare the end of the tactical recovery event.
- Stand down recovery team and have staff return to their normal job functions.
- Continue to monitor the infrastructure for potential persistency of malicious activities and inform the incident response and recovery team of any evidence.
- Finalize the metrics collected during the event.

A.3 Strategic Recovery Phase

The following steps summarize the activities performed during the strategic recovery phase.

A.3.1 Planning and Execution

- Support the various communication teams as they interact with internal users and public customers.
- Close the loop with external entities who have been involved during the tactical phase.
- Develop a plan to correct the root cause of the cyber event.
- Implement changes to strengthen the security posture of the organization.

A.3.2 Metrics

- After recovery is completed, review metrics that were collected.
- Review achievement of key milestones and assumptions that were made pre-recovery.

A. 3.3 Recovery Plan Improvement

- Use lessons learned from the recovery process to enhance the recovery plan.