



2023 CALIFORNIA PRIVACY LAW HANDBOOK



California Privacy Law Handbook

By ComplyAuto



<https://www.complyauto.com>

Introduction

Welcome to the California Privacy Law Manual, meticulously crafted by ComplyAuto for the California New Car Dealers Association (CNCDA). As a CNCDA licensed vendor for California Privacy Compliance, ComplyAuto understands the paramount importance of data privacy in the rapidly evolving automotive industry. As such, CNCDA has partnered with them to create this manual. This manual is designed to equip CNCDA members with the essential knowledge and tools to navigate the complexities of California Privacy Law and ensure a seamless integration of privacy best practices into their daily operations at the dealership. We recommend that you refer to [Appendix B](#) to find a compliance checklist and use it as a guide to follow the discussion of each of these important aspects of the CCPA.

With a focus on clarity and simplicity, this manual aims to demystify the legal jargon and help dealerships achieve and maintain full compliance with the ever-changing privacy landscape in California. We hope this manual helps in fostering a culture of data protection that respects the privacy rights of all consumers and fortifies the trust between car dealers and their valued customers.

Legal Disclaimer

This Compliance Manual is not intended as a source of legal advice nor a substitute for legal advice. Rather, this manual is intended to be a source of guidance to California new car dealers on the CCPA. The laws and regulations are subject to constant change and there may have been developments since the date of this publication (April 2023). Readers who require legal advice should contact competent counsel for further information.

Copyright

This manual, including its text, sample documents, layout, and design, is protected under the copyright laws of the United States. No part of this publication may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of both copyright holders: ComplyAuto Privacy LLC and the California New Car Dealers Association (CNCDA).

About CNCDA

The California New Car Dealers Association (CNCDA) is the nation's largest state automobile dealer association, representing over 1,200 franchised new car and truck dealers throughout California. CNCDA advances dealers' interests before government, regulatory agencies, and the courts.

CNCDA also provides many compliance resources to its dealer members, including seminars, webinars, and this compliance manual. To access many of these compliance resources, visit CNCDA Comply at www.cncda.org. Members can also call or email CNCDA's legal hotline at 916-441-2599 or legalhotline@cncda.org for basic compliance information.

About the Authors

HAO NGUYEN



Chief Legal Officer, ComplyAuto
hao@complyauto.com

Hao Nguyen has spent his entire legal career in the automotive industry. After a stint with the California New Car Dealers Association, he joined Auto Advisory Services and helped in its transition to KPA after it was acquired in 2018. While there, he provided legal support in all functions at the dealership: from sales operation and registration to service department compliance and vehicle advertising. He now furthers the interests of automotive dealers in a different capacity and brings his knowledge and expertise to ComplyAuto. He resides in Long Beach, California with his wife and dog, Buster.

CHRIS CLEVELAND



Co-Founder & CEO,
ComplyAuto
chris@complyauto.com

Chris Cleveland was the compliance director of the Galpin Automotive Group and is the Co-founder of ComplyAuto. He has spent over a decade specializing in automotive regulatory compliance and oversaw a compliance team that conducted over 40 regularly scheduled audits in the areas of sales, finance, privacy, human resources, environmental health & safety, information security, and identity theft. In his role at ComplyAuto, Chris is committed to using his dealer experience to provide practical and automated software solutions that significantly reduce the dealership's potential liability with respect to government action and private lawsuits. He resides in Utah with his wife and son.

About ComplyAuto

Built by and for dealers, ComplyAuto is a software company specializing in automating privacy and cybersecurity compliance specifically for dealerships. ComplyAuto offers a full suite of solutions to achieve compliance with state and federal privacy and cybersecurity laws, such as the revised GLBA Safeguards Rule and the California Consumer Privacy Act. This includes penetration testing, vulnerability assessments, policy builders, data mapping, electronic risk assessments, vendor risk and contract management, and much more. ComplyAuto has since expanded its products to include even more dealership compliance solutions. Visit www.complyauto.com for more details.

Table of Contents

Introduction	1
Legal Disclaimer	1
Copyright	1
About CNCDA	2
About the Authors	3
About ComplyAuto.....	3
Section 1: Background on Enactment of CCPA, CPRA, and Accompanying Regulations.....	7
California Consumer Privacy Act (CCPA).....	7
California Privacy Rights Act (CPRA)	7
Accompanying Regulations.....	7
Section 2: Applicability of the CCPA	9
Special Considerations for Dealer Groups.....	9
Reaching the 100,000 Record Threshold	9
Section 3: Definition of Consumer & Personal Information – Key Terms for Dealers.....	11
“Consumer”	11
“Personal Information”	11
Section 4: Data Mapping & Inventorying – A Critical Step for CCPA Compliance.....	14
Identification of Data	14
Identification of Sources and Business Purposes.....	14
Identification of Third Parties & Service Providers.....	15
Section 5: Requirement 1 – Notice at Collection	17
Drafting a Compliant “Notice at Collection”	17
Notice at Collection for Employees and Job Applicants	18
Methods for Providing the “Notice at Collection”.....	18
Offline or “In-Person” Collection.....	19
Online or Website Collection.....	19
Email Collection	20
Over-the-Phone Collection.....	20
SMS (or Text Message) Collection	21
Section 6: Requirement 2 – California Privacy Policy.....	22
Section 7: Requirement 3 – Vendor Contract & Risk Assessments.....	25
Service Providers and Contractors	25
Third Parties.....	25
Contractual Requirements for Service Providers and Third Parties	25
Additional Service Provider Contract Criteria.....	26
Challenges in Distinguishing Between “Service Provider” and “Third Parties”	27

Service Provider Risk Assessment and Testing Requirements.....	28
Dealing with Uncooperative Vendors.....	28
Section 8: Requirement 4 – Methods for Receiving Consumer Privacy Requests	30
Toll-Free Numbers, Online Request Portal, and Other Options	30
Authorized Agent Requests	30
Identity Verification.....	31
Section 9: Requirement 5 – Right to Opt-Out of Selling & Sharing	32
Definition of “Sale” and “Sharing”.....	32
Problems Relating to Cookies and Similar Technologies	32
Using a Compliant Cookie Consent Banner	33
Important Cookie Banner Design Considerations.....	33
Honoring Opt-Out Preference Signals	34
Responding to “Offline” Opt-Out Requests	34
Use of the “Your California Privacy Choices” Icon and Link	35
Section 10: Requirement 6 – Right to Know	36
Categories Requests.....	36
Specific Pieces Requests.....	36
Section 11: Requirement 7 – Right to Delete	38
Section 12: Requirement 8 – Right to Correct	40
Section 13: Requirement 9 – Right to Limit Certain Uses of Sensitive Information	41
Section 14: Requirement 10 – Right to Non-Discrimination.....	43
Section 15: Requirement 11 – Recordkeeping.....	44
Section 16: Requirement 12 – Cybersecurity Requirements.....	45
California Attorney General’s Reference to CIS Controls for Achieving Reasonable Security	45
Data Breach Liability Under the CCPA	45
Overlap with the Federal GLBA Safeguards Rule	45
Transmitting Data in Response to Right to Know Requests.....	46
Section 17: Requirement 13 – Employee Training	47
Identifying Applicable Personnel.....	47
Frequency of Training	47
Section 18: Requirement 14 – Disability & Foreign Language Requirements.....	48
Web Content Accessibility Guidelines (WCAG).....	48
Foreign Language Requirements	48
Section 19: Enforcement & Penalties for Noncompliance.....	49
Monetary Penalties	49
Private Right of Action.....	50
California Privacy Protection Agency (Agency)	50

Data Breaches	50
Section 20: Automakers	51
Automaker as a Third Party	51
Automakers and Third-Party Contracts.....	51
Section 21: Privacy Management Software.....	53
Questions.....	53
Appendix A – Sample Privacy Policy.....	54
Appendix B – Compliance Checklist.....	70
Appendix C – SP/C Agreement.....	74
Appendix D – Third Party Agreement	77

Section 1: Background on Enactment of CCPA, CPRA, and Accompanying Regulations

The California Consumer Privacy Act (CCPA)¹ and the California Privacy Rights Act (CPRA)² represent significant milestones in the ongoing effort to protect consumer privacy rights in the United States. This background section briefly outlines the key events and developments that led to the enactment of these landmark legislations and their accompanying regulations.

California Consumer Privacy Act (CCPA)

The CCPA was signed into law on June 28, 2018, and came into effect on January 1, 2020. It was inspired by the European Union's General Data Protection Regulation (GDPR) and was passed in response to the growing concerns about data privacy and security breaches affecting consumers in California. The CCPA grants specific rights to California residents regarding their personal information, such as the right to know, the right to delete, and the right to opt-out of the sale of their personal data. The California Attorney General enforces the CCPA, and certain businesses must comply with the law to avoid substantial fines and penalties.

California Privacy Rights Act (CPRA)

The CPRA was introduced as a ballot initiative, Proposition 24, in the 2020 California General Election and was passed by California voters on November 3, 2020. It was a signal from most California residents that they continue to prioritize their personal information and wanted businesses to be more transparent in their data collection practices. The CPRA expands and strengthens the existing CCPA framework by introducing new consumer rights, such as the right to correct inaccurate personal information and the right to limit the use and disclosure of sensitive personal information. It also establishes the California Privacy Protection Agency (Agency), which is an independent regulatory agency whose main responsibility is to enforce the CPRA. The CPRA's provisions went into effect on January 1, 2023, and enforcement is set to begin on July 1, 2023.

Accompanying Regulations

To support the implementation and enforcement of the CCPA and CPRA, the California Attorney General's Office and the Agency released a series of accompanying regulations that, together, total hundreds of pages of text. These regulations provide guidance and clarifications on various aspects of the laws, including how businesses should handle

¹ Civil Code §§ 1798.100 *et seq.*

² 11 CCR §§ 7000 *et seq.*



consumer requests, maintain their records, and provide notice of their privacy practices to the general public. The regulations are periodically updated to address evolving concerns and clarify ambiguities, ensuring that businesses remain aware of their obligations under the CCPA and CPRA. As of the publication date of this manual, the most recent set of regulations were finalized in February 2023.

Together, the CCPA, CPRA, and their accompanying regulations form the foundation of California's comprehensive data privacy framework, which aims to protect consumer rights, increase transparency, and hold businesses accountable for their data collection practices. It was the first comprehensive consumer data privacy law in America in 2018, and, as of this writing, eight other states have followed to introduce their own variation on this legislation in Colorado, Connecticut, Indiana, Iowa, Utah, Virginia, Washington, and, most recently, Montana and Tennessee.

To not confuse readers with similar sounding acronyms, since the CPRA just expands upon and modifies the CCPA, this manual will refer to the CCPA, CPRA, and their accompanying regulations as simply the “CCPA.”

Section 2: Applicability of the CCPA

According to the CCPA, a dealership must meet each of the following criteria to be considered a "business" subject to the law:³

- a. Operate for profit and do business in California;
- b. Collect, sell, or share the personal information of California residents; and
- c. Meet at least one of the following thresholds:
 - i. Have an annual gross revenue exceeding \$25 million;
 - ii. Buy, receive, sell, or share personal information of 100,000 or more California residents, households, or devices annually; or
 - iii. Derive 50% or more of its annual revenue from selling California residents' personal information.

Special Considerations for Dealer Groups

It is essential to note that dealer groups with common branding will likely be considered a single business for the purpose of determining whether the revenue and the records collected thresholds under the CCPA are met. This is based on the definition of "business" as provided in the CCPA, which includes any legal entity that controls or is controlled by a business and shares common branding.⁴ "Control" refers to the direct or indirect ownership of more than 50% of the voting interests, the ability to exercise a controlling influence over the management or direction of the entity, or the power to elect the majority of the board of directors. "Common branding" means sharing a name, service mark, or trademark that indicates a common enterprise.

As a result, dealer groups with common branding should evaluate their combined annual gross revenue and the number of personal information records collected, sold, or shared across all their affiliated entities to determine whether they meet the thresholds outlined in the CCPA. By considering the dealer group as a single business, affiliated dealerships can better assess their legal obligations under these privacy laws and ensure comprehensive compliance across the group.

Reaching the 100,000 Record Threshold

It is important to recognize that the number of personal information records shared could easily reach 100,000 or more, considering the various data storage systems utilized by a typical dealership. Dealer Management Systems (DMS), Customer Relationship Management (CRM) systems, and other digital platforms often store very large quantities of personal information, including customer contact details, purchase histories, and vehicle identification data. Additionally, it is crucial to consider the expansive definition of

³ Civil Code § 1798.140(d)

⁴ Civil Code § 1798.140(d)(2)



Personal Information (PI) under the CCPA, which includes a wide range of data elements such as identifiers, internet activity, geolocation data, and inferences drawn from personal information. With this broad definition in mind, the number of PI records shared could reach the 100,000 threshold even more rapidly. Dealerships frequently engage in retargeted advertising campaigns that involve sharing cookie data and other online identifiers with companies like Facebook and Google. This cookie data is provided to the dealership by any consenting consumer who visits their webpage and the sharing of data for advertising purposes contributes to the overall count of personal information records collected, sold, or shared.

In short, given the massive accumulation of personal information records through various data storage systems and sharing practices, such as DMS, CRM platforms, and retargeted advertising with companies like Facebook and Google, it is recommended that dealerships operate under the assumption that the CCPA may apply to them. By proactively considering the applicability of these privacy laws, dealers can implement appropriate measures to safeguard consumer data and ensure compliance with the regulations. This approach not only minimizes the risk of potential fines and penalties but also helps to build trust and confidence with customers by demonstrating a commitment to protecting their personal information.

Section 3: Definition of Consumer & Personal Information – Key Terms for Dealers

Understanding the definitions of "consumer" and "personal information" is vital for dealerships to effectively navigate the CCPA requirements. Dealerships are uniquely affected by the CCPA due to the diverse categories of personal information they collect during various customer interactions, such as sales, financing, service, and digital advertising.

“Consumer”

The CCPA broadly protects and extends rights to “consumers”, defined as a natural person who is a California resident.⁵ The term includes customers, prospective customers, employees, independent contractors, and other individuals whose personal information is collected, sold, or shared by a dealership, including as part of a business-to-business transaction. Previously the CCPA exempted employees and business-to-business transactions, but those exemptions expired on January 1, 2023.

“Personal Information”

The definition of “personal information” under the CCPA is extremely broad. It is defined as 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. Examples of personal information include, but are not limited to:⁶

1. Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol (IP) address, email address, account name, social security number, driver’s license number, passport number, or other similar identifiers.
2. Any categories of personal information that identifies, relates to, describes, or is capable of being associated with a particular individual, which includes, but is not limited to, signatures, physical characteristics or description, telephone number, state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information.⁷
3. Characteristics of protected classifications under California or federal law, including, but not limited to, veteran status and age (date of birth).

⁵ Civil Code § 1798.140(i)

⁶ Civil Code § 1798.140(v)(1)

⁷ Civil Code § 1798.80(e)

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.
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.
8. Audio, electronic, visual, thermal, olfactory, or similar information.
9. Professional or employment-related information.
10. Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act.
11. Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.
12. Sensitive personal information, which is defined as the following:
 - a. A consumer's social security, driver's license, state identification card, or passport number.
 - b. A consumer's account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account.
 - c. A consumer's precise geolocation, defined as any data that is derived from a device and that is used or intended to be used to locate a consumer within a geographic area that is equal to or less than the area of a circle with a radius of 1,850 feet.
 - d. A consumer's racial or ethnic origin, religious or philosophical beliefs, or union membership.
 - e. The contents of a consumer's mail, email, and text messages unless the business is the intended recipient of the communication.
 - f. A consumer's genetic data.
 - g. The processing of biometric information for the purpose of uniquely identifying a consumer.
 - h. Personal information collected and analyzed concerning a consumer's health.
 - i. Personal information collected and analyzed concerning a consumer's sex life or sexual orientation.

The CCPA also protects "unique identifiers", which includes cookies, pixel tags, device and mobile ad identifiers, IP addresses, and other persistent or probabilistic identifiers



that can be used to recognize a consumer or device over time and across different services.⁸

⁸ Civil Code § 1798.140(a)

Section 4: Data Mapping & Inventorying – A Critical Step for CCPA Compliance

Undertaking a comprehensive data mapping and systems inventory exercise is essential for ensuring CCPA compliance across various aspects of your dealership's data management practices. By gaining a thorough understanding of the types and sources of personal information collected, as well as how it is processed, shared, and stored, you can effectively draft compliant privacy policies, notices at collection, and vendor contracts. Additionally, a comprehensive systems inventory enables your dealership to efficiently respond to consumer requests, such as opt-outs, right to know, deletion, correction, and access requests. By investing time and effort in the data mapping and systems inventory process up front, you establish a solid foundation for your dealership's privacy compliance efforts and adherence to the CCPA's stringent requirements moving forward.

Note that a data mapping and systems inventory is also specifically required under the Federal Trade Commission's revised Safeguard Rule, effective June 9, 2023, which is covered in the ComplyAuto-CNCDA guide titled [Complying with the Revised FTC Safeguards Rule](#). A data mapping and systems inventory is the process of identifying and tracking how customer information is collected and flows through the dealership (data mapping), as well as documenting where it is stored, who it is shared with, and for which business purposes it is collected. Data mapping and system inventories can also prove beneficial in preventing and responding to data breaches and other cyberattacks.

Data breaches and cybersecurity requirements will be covered later in this manual. Below is a sample of what conducting a data mapping and systems inventory might look like.

Identification of Data

Dealers must identify the categories of personal information collected in each of their dealership's departments.⁹ This looks similar to the same categories of information described in [Section 3](#), above, but is unique to the dealer's collection and retention practices.

Identification of Sources and Business Purposes

After it is determined which categories of personal information are collected in each department, dealers should start identifying the categories of sources from which that information is collected and the business purposes for which it is used.¹⁰ Below is a sample list of sources and business purpose categories that serve as a good starting point.

⁹ Civil Code § 1798.100(a)(1)

¹⁰ Civil Code § 1798.130(a)(5)

Sample Categories of Sources:

- Advertising Networks & Agencies
- Data Brokers & Analytics Providers
- Government Entities
- Social Media Networks
- Online Lead Providers
- Credit Reporting Agencies
- Vehicle Manufacturers
- Captive Finance Companies
- Vehicle Subscription Services
- Insurance Companies
- Internet Service Providers
- Cell Phone Carriers
- Towing Companies

Sample Categories of Business Purposes:

- Auditing/Counting Ad Impressions
- Fraud/Security Incident Prevention
- Contextual & Behavioral Targeting (Retargeting Advertising)
- Customer Service
- Advertising & Marketing
- Processing & Fulfilling Orders and Transactions
- Providing Financing
- Public Health & Safety Purposes
- Defending Against Claims & Litigation

Identification of Third Parties & Service Providers

Now that the dealer has identified the categories of personal information collected, the next step is to identify and document the Third Parties and Service Providers the dealer uses to process, access, or store customer information.¹¹ Below is a sample list of vendors that may have access to customer information:

- Appraisal Tools
- Auctions & Wholesalers
- Call Tracking & Phone Solutions
- Car Rental Companies
- Chat Modules
- Check Guarantee Companies
- Consumer Defense Attorneys
- Credit Reporting & Compliance Systems
- Credit Reporting Agencies (CRAs)
- Customer Relations Management (CRM)
- Data Analytics Tools
- Dealer Management System (DMS)
- Debt Collection Agencies & Repossession Companies
- Desking Tools
- Digital Retailers & eCommerce Platforms
- Direct Mailers

¹¹ Civil Code § 1798.100(b)

- DMV Title & Registration Software
- Electronic Estimate & Invoice Tools
- Electronic F&I Menu Systems
- Email Blast Companies
- F&I Product Providers & Administrators
- Financial Institutions
- Government Entities
- Insurance Brokers
- Lien Sale Companies
- Online Service Appointment Schedulers
- Parts eCommerce Platforms
- Payment Processors & Gateways
- Payroll, Benefits & HR Software Platforms
- Records Management Companies
- Rental & Loaner Software
- Repair & Sublet Facilities
- Reputation Management Companies
- Retargeting Services
- Rideshare Companies
- Sales and F&I Consultants
- Service Communication Software
- Service Department Consultants
- Social Media Networks
- Tax Accountants and Other Professionals
- Text Messaging Tools
- Towing Companies
- Transportation Companies
- Vehicle Manufacturers
- Warranty Reimbursement Software or Services
- Website Providers

Section 5: Requirement 1 – Notice at Collection

The CCPA mandates that businesses provide a notice at the point of collection to inform consumers about the categories of personal information being collected and the purpose(s) for which it will be used.¹² The notice must be displayed conspicuously and prominently at or before collection of the consumer's personal information.¹³ The notice at collection requirement is strictly enforced, stipulating that dealers are prohibited from collecting any information not explicitly disclosed in the notice. This section outlines the notice at collection requirements and provides tips for using signage, text message disclosures, email disclosures, voice recordings, and cookie banners to comply with these privacy laws effectively.

Under the CCPA businesses must provide consumers with a notice at collection that includes:

1. A list of the categories of personal information about consumers, including categories of sensitive personal information, to be collected.
2. The purpose(s) for which the categories of personal information, including categories of sensitive personal information, are collected and will be used.
3. Whether each category of personal information identified is sold or shared.
4. The length of time the business intends to retain each category of personal information identified, or the criteria used to determine the period of time it will be retained.
5. The link to the Notice of Right to Opt-out of Sale/Sharing or, in the case of offline notices, where the webpage can be found online.
6. A link to the business's privacy policy, or in the case of offline notices, where the privacy policy can be found online.

Drafting a Compliant “Notice at Collection”

Creating a compliant Notice at Collection that complies with the six items listed above is a complex task that necessitates a thorough understanding of the dealer's data management practices. The CCPA is clear that the notice must be unique to the dealership and cannot be a general template that is not reflective of the dealer's actual collection and sharing practices. Therefore, before drafting a notice, dealers must first complete a comprehensive data mapping and systems inventory exercise (described in the [previous section](#)), which involves several crucial steps:

1. Identify all vendors involved in the collection, processing, and sharing of personal information;

¹² 11 CCR § 7012(a)

¹³ 11 CCR § 7012(d)

2. Categorize the types of personal information collected in accordance with the categories listed in [Section 3](#) of this manual;
3. Determine the vendors to whom data is shared, and classify them as third parties, service providers, or contractors, as defined under the CCPA;
4. Identify the categories of sources (e.g., digital advertising companies, lead providers, vehicle manufacturers, etc.) from which personal information is collected; and
5. Establish the specific purposes for which personal information is collected, sold and/or shared in each instance.

By conducting a comprehensive data inventory, dealers can gain a clear understanding of their data management landscape, enabling them to draft a Notice at Collection that accurately reflects their practices and complies with the CCPA requirements. Of course, the dealer must update the notice regularly as it onboards new (and leaves existing) vendors and service providers or elects to engage in new data sharing/collection activities, to ensure the notice remains accurate.

Privacy management software companies like [ComplyAuto](#) can help streamline this process by automating the data mapping and systems inventory based on dealer-specific vendor templates and management systems. For example, the system synchronizes automatically with the dealer's privacy policy and Notice at Collection, ensuring that the information stays current and accurate. By leveraging such solutions, dealers can efficiently maintain compliance with privacy regulations while minimizing the time and effort required for manual data inventory management and privacy policy disclosure.

Notice at Collection for Employees and Job Applicants

While not explicitly required by law, it is highly recommended to create a *separate* Notice at Collection specifically for job applicants and employees because the information collected in these contexts is often substantially different from the information collected from consumers. To ensure compliance, place a link to this separate notice on job application websites before collecting any personal information from applicants. In offline interactions, include a physical notice that employees can sign as part of their new hire paperwork. Since employment laws and regulations can be complex, it is important to consult with competent employment counsel to ensure that your dealership's practices align with all applicable legal requirements.

Methods for Providing the “Notice at Collection”

CCPA regulations make it clear that the above notice at collection requirements apply to the following methods of collecting personal information from consumers:¹⁴

¹⁴ 11 CCR § 7012(c)

- Offline or “in-person” collection at the dealership;
- Online collection via the dealership’s website and similar mechanisms;
- Collection via email;
- Over-the-phone collection of consumer personal information; and
- Information collected via SMS or text messages.

Below we will discuss some practical tips for satisfying the notice at collection requirement for each of these methods.

Offline or “In-Person” Collection

While the law allows for dealers to satisfy this requirement by handing out physical copies of the Notice at Collection, the use of signs is often preferred for its simplicity and efficiency. Explicitly allowed under the regulations, this preference stems from the practical challenges associated with printing lengthy notices (which are usually several pages long) and ensuring that every consumer receives a copy prior to collecting any information. By utilizing clear and conspicuous signage, dealerships can consistently and effectively convey the required information to all customers while minimizing logistical hurdles.

Some tips for compliant and effective signage include:

1. Conspicuously place the sign in each area where personal information is collected, such as reception desks, sales showrooms, parts and service counters, and your human resources department.
2. Ensure the text is easy to read with clear fonts and appropriate font sizes. We generally recommend a standard size of at least 8 ½ x 11 inches.
3. Ensure the sign is both in English and any other commonly used language at the dealerships.
4. Ensure the sign has *direct links or* QR codes (not general links to your homepage or other places where the consumer would need to navigate) to (1) the Notice at Collection and (2) your online privacy request portal where consumers can submit “do not sell/share” requests.

Online or Website Collection

By far the easiest way to ensure compliance with the online Notice at Collection requirement is to combine the proper disclosures and link to the notice in a prominent cookie consent banner displayed upon the user’s first visit to the website (we will discuss later in this manual other reasons why the cookie banner is a necessary and effective compliance tool for CCPA compliance). By implementing a cookie banner for the Notice at Collection, dealers can efficiently cover all online data collection points across their

websites without the need to place separate notices for each in-take form or other method of collection.

A cookie banner is also arguably the *only* way to cover the collection of cookies, pixel tags, and similar information, primarily because these technologies are deployed and collect information as soon as the website loads -- remember, the notice must be provided *at or before* the time information is collected. By using a cookie banner, dealers can provide immediate notice to users about their data collection practices relating to cookies and similar technologies, ensuring compliance with Notice at Collection requirements even for technologies that begin collecting information upon the page loading.

Email Collection

To satisfy the notice requirement for collection via email, dealers can include a disclosure and link to the bottom or signature line of their email correspondence. The link navigates to the dealer's privacy policy and Notice at Collection. As a general reminder, in addition to the Notice at Collection requirement, dealers must also fulfill federal CAN-SPAM disclosures, which require an "Unsubscribe" link and information identifying the dealer. Dealers may need to collaborate with their marketing vendors, CRM, and email providers to incorporate an added disclosure and link to the Notice at Collection at the bottom of their email templates.

Over-the-Phone Collection

For phone interactions, dealers can satisfy the Notice at Collection requirement by using a pre-recorded voice message that informs callers of the data collection practices and the purposes for which consumers' personal information will be collected. The message should be played at the beginning of the call before any personal information is collected. It is usually added to an existing "This call may be recorded for training purposes . . ." message. For example, the following language could be added to the recording:

Your privacy is important to us. To view the categories of personal information we collect and the purposes for which the information is used, or to exercise your rights under the California Consumer Privacy Act (CCPA), visit <insert URL>.

Dealers concerned about the length of the above disclosure could use a less conservative, but shorter version, as follows:

Visit <insert URL> to view a copy of our privacy policy and notice of collection.

Again, dealers may need to work with their phone, call tracking, and other vendors to add this custom disclosure.

SMS (or Text Message) Collection

To satisfy the Notice at Collection requirement for collection via text messages, dealers can include an added disclosure and link to their privacy policy and Notice at Collection within their initial text message that usually asks, "Reply YES to consent to texting" or "Reply STOP at any time" (this is usually provided prior to collecting any information from consumers via text message). The disclosure should mirror the language recommended for over-the-phone collection. Dealers will likely need to work with multiple vendors (e.g., CRM, service appointment schedulers, marketing companies, and other communications vendors) to ensure this language is added to their initial text message consent disclosures.

Section 6: Requirement 2 – California Privacy Policy

The CCPA requires dealers to maintain a comprehensive and up-to-date online California privacy policy that provides consumers clear and transparent information about the business's data collection and sharing practices.¹⁵ The most recent regulations provide guidance on the specific elements that must be included in a privacy policy to ensure compliance with the CCPA, and they are quite comprehensive.¹⁶ While a model privacy policy is provided in [Appendix A](#) of this manual, the specific elements required in the privacy policy are as follows:

1. Identification of the categories of personal information the business has collected about consumers in the preceding 12 months.
2. Identification of the categories of sources from which the personal information is collected.
3. Identification of the specific business or commercial purpose for collecting personal information from consumers.
4. Identification of the categories of personal information, if any, that the business has sold or shared to third parties in the preceding 12 months, and for each category of personal information, the categories of third parties to whom the information was sold or shared.
5. Identification of the specific business or commercial purpose for selling or sharing consumers' personal information.
6. A statement regarding whether the business has actual knowledge that it sells or shares the personal information of consumers under 16 years of age.
7. Identification of the categories of personal information, if any, that the business has disclosed for a business purpose to third parties in the preceding 12 months, and for each category of personal information, the categories of third parties to whom the information was disclosed.
8. Identification of the specific business or commercial purpose for disclosing the consumer's personal information.
9. A statement regarding whether or not the business uses or discloses sensitive personal information for purposes of inferring characteristics about consumers.
10. An explanation of the rights that the CCPA confers on consumers regarding their personal information, which includes the following:
 - a. The right to know what personal information the business has collected about the consumer, including the categories of personal information, the categories of sources from which the personal information is collected, the business or commercial purpose for collecting, selling, or sharing personal information, the categories of third parties to whom the business discloses

¹⁵ Civil Code § 1798.130(a)(5)

¹⁶ 11 CCR § 7011

- personal information, and the specific pieces of personal information the business has collected about the consumer;
- b. The right to delete personal information that the business has collected from the consumer, subject to certain exceptions;
 - c. The right to correct inaccurate personal information that a business maintains about a consumer;
 - d. The right to opt-out of the sale or sharing of their personal information by the business;
 - e. The right to limit the use or disclosure of sensitive personal information by the business;
 - f. The right not to receive discriminatory treatment by the business for the exercise of privacy rights conferred by the CCPA, including the right of an employee, job applicant, or independent contractor not to be retaliated against for the exercise of their CCPA rights.
11. An explanation of how consumers can exercise their CCPA rights and what consumers can expect from that process, which includes the following:
- a. An explanation of the methods by which the consumer can exercise their CCPA rights;
 - b. A notice describing the customer's right to stop the selling/sharing of data, use of sensitive personal information, and a link to the portal where consumers can submit privacy requests exercising those rights;
 - c. Instructions for submitting a request under the CCPA, including any links to the dealer's online request form or portal for making such a request;
 - d. A general description of the process the business uses to verify a consumer request to know, request to delete, and request to correct, including any information the consumer must provide;
 - e. Explanation of how an opt-out preference signal will be processed for the consumer (i.e., whether the signal applies to the device, browser, consumer account, and/or offline sales, and in what circumstances) and how the consumer can use an opt-out preference signal;
 - f. Instructions on how an authorized agent can make a request under the CCPA on the consumer's behalf;
 - g. A contact (i.e. an email or a phone number) for questions or concerns about the business's privacy policies and information practices using a method reflecting the manner in which the business primarily interacts with the consumer.
 - h. The date the privacy policy was last updated.

As with the Notice at Collection requirements discussed earlier, crafting a compliant CCPA privacy policy is a highly complex and intricate endeavor that necessitates referencing your data mapping and systems inventory to devise multiple charts illustrating



the various types of information collected. Dealers need to consider the various scenarios in which information is collected, the parties it is shared with, the sources of collection, and the purposes for which it is used. Additionally, several other technical and legal disclosures must be included. As noted earlier, please consult the model privacy policy provided in [Appendix A](#).

Section 7: Requirement 3 – Vendor Contract & Risk Assessments

CCPA regulations delineate specific requirements for “Service Providers”, “Contractors” and “Third Parties”. Each of these entities are legally defined terms in the CCPA, and it is crucial for dealers to understand the distinctions between these three types of entities because different contractual requirements apply depending on the entity’s designation.

Service Providers and Contractors

Service Providers perform specific services on behalf of a dealer and process personal information solely for the dealer's purposes.¹⁷ They are not allowed to use the consumer’s personal information for their own marketing or business purposes, resell the data, or combine it with data that it has collected from other sources for analytical purposes. Some obvious examples of Service Providers for dealers include DMS providers, CRM software, appraisal tools, payroll, and HR software that process consumer personal information on behalf of the dealer. The difference in the definition of “Contractor” is a bit more subtle as both terms generally refer to entities that process personal information on behalf of the business for specific purposes. However, at the time of this manual's publication, the difference between the two terms has not led to any significant legal implications. As such, for the purposes of this manual, they will be treated the same.

Third Parties

Under the CCPA, Third Parties are defined in the negative as those who are *not* classified as Service Providers.¹⁸ They often receive personal information from a dealer but may use the information for their own marketing and business purposes, resell the data, or combine it with data collected from other sources for analytical purposes. Examples of third-party entities for dealers often include digital advertising & retargeting companies, data analytics software, and vehicle manufacturers.

Contractual Requirements for Service Providers and Third Parties

The CCPA regulations require both Service Providers and Third Parties to sign a specific written agreement outlining their respective roles and responsibilities.¹⁹ Under the latest regulations, the use of generic templates to satisfy the contract requirements is explicitly prohibited. Instead, in each dealership contract, Service Providers and Third Parties must list the specific purposes for which they collect, sell, or share personal information on the dealership's behalf.²⁰ Moreover, Service Providers and Third Parties must agree not to use the information outside of the specified purposes. It is important to note that the

¹⁷ 11 CCR § 7050(a)

¹⁸ Civil Code § 1798.135(ai)

¹⁹ 11 CCR §§ 7051, 7053

²⁰ 11 CCR §§ 7051(a)(2), 7053(a)(1)

permissible “business purposes” for which a Service Provider can process personal information is defined by law.²¹ Therefore, the contract should list the applicable purposes itemized under the CCPA. Third Parties must list the other “non-business purposes” for which they collect information (i.e., purposes not defined as business purposes and therefore disqualify them from being service providers). In addition to listing the specific purposes for collecting consumer personal information, both Service Provider and Third Party contracts must contain the provisions requiring the Service Provider or Third Party to do the following:²²

- Comply with all applicable sections of the CCPA by providing the same level of privacy protection as required by the dealer;
- Cooperating with the dealer in responding to consumer requests, implementing reasonable security procedures;
- Upon receiving written notice from the dealer, take appropriate steps to stop and remediate the Service Provider’s unauthorized use of the personal information;
- Cooperate with the dealer in responding to and complying with consumers’ requests made pursuant to the CCPA and to implement reasonable security procedures and practices appropriate to the nature of the personal information received from, or on behalf of, the dealer to protect the personal information from unauthorized or illegal access, destruction, use, modification, or disclosure; and
- Notify the dealer as soon as practicable after it determines it can no longer meet its obligations under the CCPA.

Refer to [Appendix C](#) and [Appendix D](#) to find samples of each of these Service Provider and Third-Party agreements. It is important to remember that the agreements must be unique to the vendor that dealers are working with. Said in another way, each of these agreements will be different from one another depending on what kinds of services the vendor provides for the dealer.

Additional Service Provider Contract Criteria

Service Provider contracts must also prohibit the Service Provider from doing the following:²³

- “Selling” or “sharing” personal information it collects pursuant to these contracts as those terms are defined under the CCPA.
- Retaining, using, or disclosing the consumer’s personal information for any purpose other than for the specific purpose of performing the business purposes specified in the contract for the dealer, or as otherwise expressly permitted by the CCPA or accompanying regulations.

²¹ Civil Code § 1798.140(e)

²² 11 CCR §§ 7051(a)(2)-(3) and (6)-(9), 7053(a)(1)-(6)

²³ Civil Code § 1798.140(ag)(1)(D); 11 CCR §§ 7051(a)(1), (4)-(5).

- Retaining, using, or disclosing personal information outside of the direct business relationship between Service Provider and dealer.
- Combining the consumer's personal information that the Service Provider receives from, or on behalf of, the dealer with personal information that it receives from, or on behalf of, another business, or collects from its own interactions with consumers, except as otherwise expressly permitted by the CCPA or accompanying regulations.
- Using personal information to engage in retargeting advertising or cross-contextual behavioral advertising.

Dealers should make special note of the first and last bullet points above. The CCPA is explicit in stating that Service Providers are restricted from engaging in retargeted advertising or cross-context behavioral advertising because engaging in these activities (which constitute “selling” or “sharing”) would classify them as Third Parties.

Challenges in Distinguishing Between “Service Provider” and “Third Parties”

Distinguishing between a Service Provider and a Third Party can often be a complex task that requires careful analysis. The CCPA defines these entities based on their relationship with the dealer and the purposes for which they use the collected personal information. However, the lines can be blurred in certain situations, necessitating a thorough examination of the vendor's practices and the specific services they provide. For example, distinguishing between a Service Provider and a Third Party under the CCPA involves analyzing whether the dealer may be “selling” or “sharing” personal information, as these activities have specific definitions under the law. “Selling” is broadly defined as transferring personal information for monetary or other valuable consideration,²⁴ while “sharing” refers to disclosing personal information for cross-context behavioral advertising purposes.²⁵

The general consensus is that most dealers engage in “selling” and “sharing” activities in some capacity, such as providing data to vehicle manufacturers, retargeting advertising companies, data analytics firms, or by entering into data sharing agreements where the dealer provides consumer information in exchange for manufacturer incentives, benefits, promotional services, software reimbursement, or other valuable services. Understanding the nature of these relationships and the flow of data is crucial to accurately categorize vendors as Service Providers or Third Parties since the vendor will always be categorized as a Third Party if the dealer is deemed to be “selling” or “sharing” data with them.

To further complicate matters, the CCPA includes exemptions for certain types of vendors and information collected. For example, consumer reporting agencies (e.g., Equifax, Transunion, and Experian) that provide credit reports to dealers for financing purposes

²⁴ Civil Code § 1798.140(ad)

²⁵ Civil Code § 1798.140(ah)

are exempt from the CCPA when they collect, maintain, or sell personal information as part of a consumer report as this information is already regulated under the Fair Credit Reporting Act (FCRA).²⁶ Another example is vehicle manufacturers when they receive warranty or recall information from dealers; they are exempt from the CCPA when using that information to conduct warranty or recall-related repairs, as it falls under an exception for vehicle repair and warranty information.

Additionally, certain government entities may be exempt from the CCPA under specific circumstances. For instance, when dealers share personal information with the Department of Motor Vehicles (DMV) for vehicle registration purposes, this information is regulated under the Driver's Privacy Protection Act (DPPA) and may be exempt from the CCPA.²⁷

Finally, when dealers share financial information with the Internal Revenue Service (IRS) to comply with tax reporting requirements such information sharing might be exempt from the CCPA due to its status as a necessary part of fulfilling legal obligations.²⁸

Given the intricacies involved in differentiating between Service Providers and Third Parties and identifying the applicable exemptions, it is crucial for dealers to seek professional guidance and carefully analyze their relationships with vendors to ensure CCPA compliance.

Service Provider Risk Assessment and Testing Requirements

Dealers are now required to complete manual reviews, automated scans, internal or third-party assessments, or other testing of Service Providers at least once every twelve (12) months. The assessment or test must be designed to demonstrate the Service provider's compliance with their contractual requirements and CCPA regulations as described above. Because it remains unclear how an "automated scan" could determine a Service Provider's compliance with the requirements described in this section, dealers might opt to send a risk assessment questionnaire to their Service Providers once per year that asks questions designed to confirm their compliance with applicable CCPA regulations.

Dealing with Uncooperative Vendors

If a Service Provider or Third Party refuses to sign a CCPA agreement or complete the aforementioned risk assessment, it is the dealer who faces potential risks and consequences. The CCPA regulations explicitly state that a dealer's failure to secure signed agreements from these parties can be used as evidence in any enforcement actions.²⁹ Such evidence may be used to determine whether the dealer did not conduct the required due diligence, was negligent in sharing personal information with the vendor, or even knew that the vendor was not in compliance with the CCPA and still provided the

²⁶ Civil Code § 1798.145(d)

²⁷ Civil Code § 1798.145(f)

²⁸ Civil Code § 1798.145(a)(1)

²⁹ 11 CCR § 7051(c)



information anyway. In light of these strict regulations, dealers must carefully evaluate their relationships with uncooperative vendors. Dealers should weigh the risks of continuing to do business with vendors who refuse to sign CCPA agreements against the potential consequences to them for noncompliance because, after all, the responsibility falls on the dealer and rarely do vendors bail them out in these situations. Ultimately, it may be in the dealer's best interest to discontinue relationships with vendors that are unwilling to comply with the CCPA's requirements to mitigate potential legal and financial risks.

Other situations may arise where a Service Provider or Third Party will claim that the existing Master Service Agreement (or a Terms of Service) that you have completed with them fulfills the requirement. If this is the case, then it is encouraged that the dealer works with their attorneys or outside counsel to ensure that these documents fulfill these requirements. Keep in mind that this requirement is new for 2023 so any document that was signed prior to this year may not be sufficient.

Section 8: Requirement 4 – Methods for Receiving Consumer Privacy Requests

As a dealer, it is essential to establish proper channels for receiving consumer privacy requests in compliance with the CCPA. This section will cover the key aspects of receiving and processing consumer privacy requests to ensure that dealers comply with the necessary requirements under the CCPA.

Toll-Free Numbers, Online Request Portal, and Other Options

The law requires dealers to provide at least two methods for consumers to submit their privacy requests. A toll-free number plus, either:

1. an online interactive request portal, email address, or
2. a physical mailing address must be provided.

The online request portal is the most popular choice as it offers a more user-friendly and accessible experience for consumers. It can also help the dealer significantly automate the workflow and processing of requests in a way that is limited by email and regular mail such as authenticating or verifying the request.

Authorized Agent Requests

Dealers must also allow authorized agents to submit privacy requests on behalf of consumers.³⁰ Authorized agents may be designated through a power of attorney or another signed document, but dealers must be careful not to require the power of attorney or notarization methods unless they are prepared to pay for that service. To verify the agent's authorization to act on the consumer's behalf, dealers must follow specific procedures depending on whether the proof provided is a power of attorney or other signed document.

If an agent provides a power of attorney signed by the consumer ("principal") that purports to give the agent authorization to submit the request on the principal's behalf, the dealer should require that the agent provide information reasonably necessary or appropriate to identify the agent and principal and to facilitate the request.³¹ This includes, but is not limited to, identification of the agent and principal and the current and permanent residence addresses of the principal. The dealer should also verify the authenticity of the document. There are generally three ways to verify the legitimacy of a power of attorney document:

³⁰ 11 CCR § 7063

³¹ Probate Code §§ 4300 *et seq.*

1. *Contact the public notary (recommended)* - Most power of attorney documents are notarized. The presence of a notary's stamp and signature may be enough evidence that the power is a legitimate document. However, if the dealer is concerned about the authenticity of the document, the dealer can run an internet search for the public notary and call them directly to ask whether the stamp on the document is the notary's official seal and whether they have a record of notarizing that document. Notaries are required by law to keep a journal of all their transactions.
2. *Contact the witnesses* - As an alternative to notarizing the document, California allows a power of attorney to be authenticated by two adult witnesses who watched the principal sign the document that granted authority to the agent. If this is the case, consider contacting the witnesses at their listed addresses, emails or phone numbers to verify that they witnessed the signing of the document by the principal.
3. *Contact the principal* - If you can verify that the consumer's address matches your existing records, consider contacting the consumer directly at the listed address to verify that he or she has in fact granted power of attorney to the agent.

If the agent provides some other signed permission from the consumer that is *not* a power of attorney, the dealer should require that consumer do two things: (1) verify their identity directly with the dealer, through a combination of SMS (text message) verification, email verification, and one or more questions regarding the consumer's particular interaction or transaction with the dealership that is then matched against the dealers own internal records for consistency and (2) confirm that he or she provided the authorized agent permission to submit the request.

Identity Verification

When processing privacy requests, dealers must take appropriate steps to verify the consumer's identity.³² It is important *not* to request information that is more sensitive than necessary for the type of request. For example, requesting government-issued IDs or using facial recognition technology can lead to legal trouble. The verification process should also not be overly burdensome for the consumer.

The following sections of this manual will describe the appropriate identity verification requirements for each request in detail.

³² 11 CCR § 7062

Section 9: Requirement 5 – Right to Opt-Out of Selling & Sharing

The CCPA grants consumers the right to opt-out of the sale and sharing of their personal information.³³ This right is arguably the most important aspect of the CCPA as it constitutes over 90% of all requests submitted by consumers and is the most actively enforced by the Attorney General. This section explores the various aspects of the right to opt-out, including its definition, problems relating to cookies, and methods for honoring opt-out requests.

Definition of “Sale” and “Sharing”

As described earlier in this manual, the term “selling” is broadly defined as transferring personal information for monetary or other valuable consideration, while “sharing” refers to disclosing personal information for cross-context behavioral advertising purposes (e.g., targeted advertising).³⁴ Given these broad definitions, the general consensus is that almost all dealers engage in “selling” and “sharing” activities in some capacity, including providing data to vehicle manufacturers, retargeting advertising companies, and data analytics firms. Dealers even enter into data sharing agreements where the dealer provides consumer information to the manufacturer in exchange for manufacturer-based incentives, benefits, promotional services, software reimbursement, or other valuable services.

Problems Relating to Cookies and Similar Technologies

Third-party tracking cookies and similar technologies, such as those deployed by Google Ads and Facebook (Meta) Pixel for targeted advertising, are considered a “sale” or “sharing” of information and are therefore subject to the CCPA’s right to opt-out. Nearly all dealership websites deploy such cookies and similar tracking technologies, which collect information that is shared with third parties to build profiles, serve ads, and personalize consumers’ experiences across websites. Without a properly functioning stop gap to verify the consumer’s choice, such as a cookie consent banner, these cookies and tracking technologies deploy automatically upon the consumer visiting the dealer’s website.

As a reminder, under the CCPA, the definition of “personal information” includes a persistent identifier that can be used to recognize a consumer or a device that is linked to a consumer, including, but not limited to, a device identifier; an Internet Protocol address; cookies, beacons, pixel tags, mobile ad identifiers, or similar technologies.³⁵ Personal information also includes internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information

³³ Civil Code § 1798.120

³⁴ Civil Code §§ 1798.140(ad) and (ah)

³⁵ Civil Code § 1798.140(v)(1)

regarding a consumer's interaction with an internet website, application, or advertisement. Therefore, in the context of cookies, "personal information", such as tracking pixels, browsing history, and website interactions, that are shared with a third party in exchange for the monetization of ads, retargeting, analytics, or other "valuable services" is in fact a "sale" of information under the CCPA. Further, the CCPA's definitions of "sharing" and "cross-contextual behavioral advertising" seems to explicitly target third-party tracking cookies and make them subject to opt-out rights under the CCPA.³⁶

The problem is that it is extremely difficult, if not impossible in some cases, to effectively opt a customer out of the collecting and sharing of data via cookies and similar technologies once the cookie, pixel, or script has already deployed upon the user first visiting the website, particularly since some third parties cookie/script providers do not even support a subsequent opt-out capability. The question then becomes how a dealer who utilizes third-party tracking cookies can effectively comply with consumer opt-out requests.

Using a Compliant Cookie Consent Banner

The most effective method for solving the issue described above is a compliant cookie consent banner. Cookie consent banners rely on an exception to the definition of "sale" and "sharing" where information is collected and shared with the express consent and direction of the consumer. If the user accepts, the collection and sharing will not be considered "selling" or "sharing" under the CCPA.³⁷ Therefore, a well-designed cookie banner will conspicuously disclose that the website will collect and share such information with third-party advertisers if (and only if) the user selects the "Accept" button. If the user selects the "Decline" button, the cookie banner will be programmed to block or prevent certain third-party tracking cookies and similar technologies from loading in the first place, thereby solving the dilemma of "after-the-fact" opt-outs as described above.

Important Cookie Banner Design Considerations

California regulators quickly recognized that many businesses were implementing cookie banners on their websites that were designed in a way to coerce or trick consumers into accepting cookies. Therefore, several regulations related to these so-called "dark patterns" have been promulgated to prohibit these types of practices.³⁸ Examples of prohibited dark patterns include the following:

- Forcing the user to interact with the cookie banner before they can view or browse the dealership's website (i.e. preventing access or "graying out" the underlying website until the consumer makes a choice on the cookie banner pop-up).
- Failing to provide a symmetrical "Accept" and "Decline" button in the same size.

³⁶ Civil Code § 1798.135(k)

³⁷ Civil Code § 1798.140(ad)(2)(A)

³⁸ 11 CCR §§ 7004(b) and (c)

- Providing an “Accept” and either a “More Settings”, “Preferences”, “Ask Me Later” or similar button designed to make it easier for the user to accept than to decline.
- Requiring more steps to decline than to accept cookies.
- Confusing language for opt-out choices or the use of double negatives.
- Manipulative language or design patterns, such as telling the consumer they will miss out on discounts or other benefits by not selecting “Accept,” such as “No, I do not want to save 15% on my next purchase.”

Dealers should be *very* wary of default or “out-of-the-box” cookie banners that may not comply with these standards as many banners load all cookies regardless of the user's choice. Not only could this violate the CCPA, but one can argue that it is an unfair and deceptive practice in implying to the consumer that specific information will not be sold or shared, while still doing so. A well-designed cookie banner will also incorporate language to satisfy the Notice at Collection requirements outlined in [Section 5](#) of this manual.

Honoring Opt-Out Preference Signals

Your cookie banner must also honor standardized opt-out preference signals, including the Global Privacy Control (GPC). Honoring such signals is specifically required by the CCPA.³⁹ An opt-out preference signal is a privacy preference feature in some web browsers and browser plug-in or add-on tools that tells a website that a user does not want their online activity to be tracked or their information sold or shared. It consists of a setting or extension in the user's browser or mobile device and acts as a mechanism that dealers' websites can use to honor the consumer's privacy settings. The GPC and similar opt-out preference signals are available for an increasing number of browsers and browser extensions. More information about GPC can be found at <https://globalprivacycontrol.org/>. Dealers should also consider complying with the popular Do-Not-Track (DNT) signal standard. More information about DNT can be found at <https://allaboutdnt.com/>. When a dealership's website detects an opt-out preference signal, it should automatically block third-party tracking cookies that could constitute the “selling” or “sharing” of personal information and display a message to the visitor in the cookie banner that the signal has been detected and honored.

Responding to “Offline” Opt-Out Requests

While the majority of this section has focused on opt-out requests with respect to the online collection of personal information via cookies and similar technologies, equally important is honoring information collected through other methods. When a customer submits an opt-out request that isn't automatically handled using the cookie consent banner or opt-out preference signal, the dealer must comply with the request by ceasing to sell to and/or share with third parties as soon as feasibly possible, but no later than

³⁹ 11 CCR § 7025

fifteen (15) business days from the date that the business receives the request.⁴⁰ In the dealer context, this usually involves manually marking a “do not share” and “do not sell” button in the CRM, DMS, and any other systems that share or push data to Third Parties. The CCPA also requires that the dealer then notify all downstream Third Parties of the request to whom the consumer’s information has been shared, directing them to comply with the request and to notify any parties to whom they have made the consumer’s information available.⁴¹

Note that a CCPA opt-out request does not cover general marketing communications with customers, which is covered under other federal and state laws. Therefore, it is normally not necessary to respond to a CCPA opt-out request by opting the customer out of email, text, or phone communications.

With respect to identity verification requirements, an opt-out request is considered a non-verifiable consumer request and must be honored unless the dealer has reason to believe it is fraudulent.⁴²

Use of the “Your California Privacy Choices” Icon and Link

Dealers must also include a specific icon and link titled “Your California Privacy Choices” that appears somewhere conspicuously on the dealerships’ homepage and the footer of the website. The link must go directly to the dealer’s online consumer privacy portal (not the privacy policy nor the Notice at Collection) where the consumer can exercise their CCPA rights.⁴³ While dealers can technically choose an alternative link titled “Do Not Sell My Personal Information”, for both practical and legal reasons, the former is usually preferred. The icon shown below was specifically designed by regulators and therefore cannot be deviated from in terms of style or type:⁴⁴



Your California Privacy Choices

⁴⁰ 11 CCR § 7026(f)(1)

⁴¹ 11 CCR § 7026(f)(2)

⁴² 11 CCR § 7026(d)

⁴³ 11 CCR § 7015

⁴⁴ 11 CCR § 7015(b)

Section 10: Requirement 6 – Right to Know

Under the CCPA, the “Right to Know” describes two separate request types: a “categories” and “specific pieces” request. Each of these types have different identity verification, response, and processing requirements.⁴⁵

Categories Requests

Under a categories request, consumers can ask businesses to generally disclose the categories of personal information collected, the categories of sources from which the information was collected, the business or commercial purpose for collecting or selling the information, and the categories of third parties with whom the business has shared personal information over the past twelve (12) months of the date of the request.⁴⁶ Additionally, consumers may request that the business provide personal information that it collected beyond the 12-month period as long as the personal information was collected on or after January 1, 2022. The business must fulfill the request unless it is either impossible or would involve disproportionate effort.⁴⁷

The response to a categories request is usually displayed in the form of a table with disclosures showing each of the categories collected and shared. Dealers must initially acknowledge the categories request within ten (10) business days and respond within forty-five (45) calendar days from the date of receipt.⁴⁸ If necessary, dealers can extend the deadline by an additional forty-five (45) calendar days, but they must notify the consumer of the extension within the initial 45-day period.⁴⁹

Dealers must verify the consumer's identity to a "reasonable degree of certainty" in these categories requests, which includes matching at least two data points provided by the consumer with data points maintained by the dealer.⁵⁰ See [Section 3](#) and [Section 4](#) of this manual for sample categories that a dealer might consider when responding to a categories request.

Specific Pieces Requests

Under a specific pieces request, consumers can ask businesses to provide them with the specific pieces of personal information collected about them.⁵¹ Unlike a categories request, the dealer must provide the customer's *actual* personal information, such as their full name, date of birth, address, purchase history, etc. It is for this reason that a “specific pieces” request is sometimes referred to as a “data portability” or “access” request. Like

⁴⁵ Civil Code §§ 1798.110, 1798.115

⁴⁶ Civil Code §§ 1798.110(a)(1)-(4); 11 CCR § 7024(h)

⁴⁷ 11 CCR § 7025(h)

⁴⁸ 11 CCR § 7021(b)

⁴⁹ Civil Code § 1798.145(h)(1); 11 CCR § 7021(b)

⁵⁰ 11 CCR § 7062(b)

⁵¹ Civil Code § 1798.110(a)(5)

categories requests, dealers must initially acknowledge the request within ten (10) business days and then respond within forty-five (45) calendar days from the date of receipt and can extend the deadline by an additional forty-five (45) calendar days if necessary.⁵²

Dealers must verify the consumer's identity to a "reasonably *high* degree of certainty" in these specific pieces requests, which includes matching at least *three* pieces of personal information provided by the consumer with data points maintained by the dealer, and requiring a declaration signed under penalty of perjury that the requestor is the consumer whose personal information is the subject of the request.⁵³

If a business cannot verify the identity of the requestor for a specific pieces request, it cannot simply reject the request, but rather, must "downgrade" the request and treat it as if it were a categories request and provide the consumer with the appropriate response.⁵⁴

Regarding the information that must be provided in response to a specific request, the dealer must search all of their physical and electronic records (e.g., hardcopies, files, the DMS, CRM, etc.) and provide any information defined as "personal information" in [Section 3](#) of this manual. However, there are some exceptions where the information does not have to be provided, including the following:⁵⁵

- Certain pieces of information that pose a high risk of being used for fraud or identity theft, including bank account numbers, credit and debit card numbers, medical information, health insurance information, biometric data, government issued identification information, and social security numbers.
- Information where the time and resources expended to provide it outweighs the reasonably foreseeable impact to the consumer by not responding.
- Information in an unsearchable or inaccessible format that is used solely for compliance purposes.
- Information covered under the Fair Credit Reporting Act (FCRA), such as the information obtained from and reported to consumer credit reporting agencies.
- Information covered under the Driver's Privacy Protection Act (DPPA), such as motor vehicle and DMV records like titles, registrations, permits, and identification cards.
- Information covered under the Gramm-Leach-Bliley Act (GLBA), such as information collected for the purposes of extending credit or arranging for vehicle financing/leasing for personal, family, or household use.

⁵² Civil Code § 1798.145(h)(1); 11 CCR § 7021(b)

⁵³ 11 CCR § 7062(c)

⁵⁴ 11 CCR § 7024(a)

⁵⁵ Civil Code § 1798.145; 11 CCR § 7024

Section 11: Requirement 7 – Right to Delete

The CCPA grants consumers the right to request that their data be permanently and completely deleted from all of the dealer's existing systems (excluding archived backups).⁵⁶

Upon receiving a deletion request, dealers have ten (10) business days to initially acknowledge the request and forty-five (45) calendar days to respond. If necessary, dealers can extend the response deadline by an additional forty-five (45) calendar days, provided they notify the consumer of the extension within the original 45-day response period.⁵⁷

When a dealer receives a valid deletion request, it must delete the information itself (if possible) and notify all of its Service Providers and Third Parties who have received the consumer's personal information from the dealer. The dealer must then direct these entities to delete the consumer's personal information unless a legal exception applies. Dealers, Service Providers, and Third Parties may not need to delete the consumer's information if the following exceptions apply:⁵⁸

- Information where the time and resources expended to delete it outweighs the reasonably foreseeable impact to the consumer by not complying.
- Information covered under the Fair Credit Reporting Act (FCRA), such as the information obtained from and reported to consumer credit reporting agencies.
- Information covered under the Driver's Privacy Protection Act (DPPA), such as motor vehicle and DMV records like titles, registrations, permits, and identification cards.
- Information covered under the Gramm-Leach-Bliley Act (GLBA), such as information collected for the purposes of extending credit or arranging for vehicle financing/leasing for personal, family, or household use.
- Personal information exempt from deletion under the CCPA because it is maintained to comply with a legal obligation, such as record retention requirements.
- Personal information exempt from deletion under the CCPA because it is maintained solely for internal uses that are reasonably aligned with consumer expectations based on their relationship with our dealership.
- Personal information exempt from deletion under the CCPA because it is maintained to detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity.

⁵⁶ Civil Code § 1798.105; 11 CCR § 7022(b)(1)

⁵⁷ Civil Code § 1798.130(a)(2)(A); 11 CCR § 7021(b)

⁵⁸ Civil Code § 1798.145; 11 CCR § 7022(f)

- Personal information exempt from deletion under the CCPA because it is maintained to complete the transaction for which the personal information was collected, fulfill the terms of a written warranty, service contract, or product recall conducted in accordance with federal law, provide a good or service requested or reasonably anticipated within the context of an on-going business relationship, or otherwise perform or fulfill an existing contract.

Keep in mind that when relying on one of the exemptions above, the dealer must clearly state the specific exemption in their response to the consumer and a detailed explanation of the reason for not deleting the particular category of personal information.⁵⁹ If the dealer denies the consumer's request to delete, the dealer must ask the consumer if they would like to opt-out of the sale or sharing of their personal information in the denial response with the applicable link or instructions.⁶⁰

Dealers must verify the identity of the requesting consumer to ensure the security and accuracy of the deletion request before processing it. The level of verification should be proportional to the sensitivity of the personal information being handled and the potential risk of harm to the consumer if the information is deleted in error or obtained by an unauthorized person. The verification process should involve matching at least two or three (depending on the sensitivity of the information) pieces of personal information provided by the consumer with data points maintained by the dealer.

⁵⁹ 11 CCR § 7023(f)(1)

⁶⁰ 11 CCR § 7022(g)

Section 12: Requirement 8 – Right to Correct

The CPRA amended the CCPA to mirror other state privacy laws by giving consumers the additional right to have inaccurate information corrected.⁶¹ Upon receiving a correction request, dealers have ten (10) business days to initially acknowledge the request and forty-five (45) calendar days to respond. If necessary, dealers can extend the response deadline by an additional forty-five (45) calendar days, provided they notify the consumer of the extension within the original 45-day response period.⁶²

Upon receiving a request to correct inaccurate information, the dealership may require documentation evidencing the inaccuracy to make a determination of whether to update its systems with the correct information.⁶³ If the dealer determines that the information is indeed inaccurate, it must notify all downstream Service Providers to whom the information has been shared to correct their records as well.⁶⁴

To efficiently process these right-to-correct requests, dealers should consider adding functionality to their online privacy request portal that lists all possible specific pieces of personal information that a consumer may want to correct. For each item, the portal should provide fields for entering the inaccurate data, the correct data, and an option to upload supporting documentation as proof of the inaccuracy.

The right to correct personal information is subject to the same exemptions as those applicable to deletion requests. Additionally, the dealer can deny the request if there is a good-faith, reasonable, and documented belief that a request to correct is fraudulent or abusive.

Much like a specific pieces request, any documentation or information collected as part of a correction request must be securely stored and transmitted. Regarding identity verification requirements, dealers should follow the same process outlined above for deletion requests.

⁶¹ Civil Code § 1798.106

⁶² Civil Code § 1798.130(a)(2)(A); 11 CCR § 7021(b)

⁶³ 11 CCR § 7023(d)

⁶⁴ 11 CCR § 7023(c)

Section 13: Requirement 9 – Right to Limit Certain Uses of Sensitive Information

The right to limit applies specifically to the use and disclosure of sensitive personal information (defined in [Section 3](#)) for the purpose of inferring characteristics about consumers.⁶⁵ It does not broadly apply to *any* use of sensitive personal information.⁶⁶ For example, the collection of a social security number for the purpose of vehicle financing and identity verification would not be subject to this right unless it is also used for the purpose of inferring characteristics about the consumer.

"Inferring characteristics" relates to the process of drawing conclusions about a consumer's attributes, preferences, or behavior based on the analysis of their personal information. According to the California Office of the Attorney General's Opinion No. 20-303, this process typically involves using algorithms, statistical models, or other data analysis techniques to identify patterns or correlations within the collected data, such as a consumer's location history or movement patterns. The inferred characteristics may relate to a consumer's interests, lifestyle, financial situation, or other aspects that could be used to profile or target them for specific purposes, such as marketing, advertising, or personalized services. In the context of precise geolocation data (which is specifically defined as "sensitive personal information" subject to the right to limit), dealers might infer characteristics like the consumer's place of residence, preferred shopping locations, frequently visited places (including competing dealerships), or commute patterns.

Car dealerships often employ geotargeting, geofencing, and other advertising strategies based on the collection of customers' precise geolocation data. These practices may be implicated under the right to limit if the dealership is using this sensitive personal information to infer characteristics about consumers for targeted advertising purposes.

Dealerships may also encounter issues with the right to limit when handling other categories of sensitive personal information, such as Social Security Numbers (SSN). For instance, if a dealership uses a customer's SSN to infer their creditworthiness or qualification for financing (e.g., pre-approved offers of credit) or to identify likely lease renewal customers based on payment histories, this practice may be subject to the right to limit.

Dealers must comply with the request to limit by ceasing to use or disclose the consumer's sensitive personal information for the purpose of inferring characteristics as soon as practicable, but no later than fifteen (15) business days from the date the business receives the request.⁶⁷ Much like CCPA opt-out requests, this usually involves the dealer manually marking a "limit use of sensitive data" checkbox or button in the CRM, DMS, and other systems that share or push data to Third Parties.

⁶⁵ Civil Code § 1798.121(a)

⁶⁶ Civil Code § 1798.121(d)

⁶⁷ 11 CCR § 7027(g)(1)



The CCPA also requires that the dealer then notify all downstream Service Providers and Third Parties of the request to whom the consumer's information has been shared, directing them to comply with the request and to notify any parties to whom they have made the consumer's information available.⁶⁸ Therefore, in order to comply with a request to limit, dealers must first identify all of the vendors that use or disclose sensitive personal information for the purposes described above. Sample vendor notifications are provided at the conclusion of this manual.

With respect to identity verification requirements, a request to limit is considered a non-verifiable consumer request and must be honored unless the dealer has reason to believe it is fraudulent.⁶⁹

⁶⁸ 11 CCR § 7027(g)(2)

⁶⁹ 11 CCR § 7027(e)

Section 14: Requirement 10 – Right to Non-Discrimination

The CCPA and its accompanying regulations emphasize the importance of protecting consumers' right to non-discrimination.⁷⁰ This right ensures that businesses do not unfairly discriminate against consumers who exercise their privacy rights under these regulations. In practice, this means that dealerships and other businesses are prohibited from:

- Denying goods or services to consumers who exercise their privacy rights.
- Charging different prices or rates for goods or services, including through the use of discounts or other benefits, to consumers who exercise their privacy rights.
- Providing a different level or quality of goods or services to consumers who exercise their privacy rights.
- Suggesting that consumers who exercise their privacy rights will receive a different price or rate for goods or services, or a different level or quality of goods or services.

⁷⁰ Civil Code § 1798.125; 11 CCR § 7028

Section 15: Requirement 11 – Recordkeeping

Businesses must maintain a record of all requests it has received pursuant to the CCPA and how they have responded, either fulfilling them or denying them, for at least twenty-four (24) months.⁷¹ Reasonable security procedures and practices must be observed in maintaining these records.

Aside from these requirements that pertain specifically to the requests, the CCPA encourages businesses to purposely collect personal information and delete personal information in which there is no longer a need to retain the information. Also known as “data minimization,” the CCPA limits the scope in the kinds of personal information a business collects, uses, discloses or retains to the information that is reasonably necessary and proportionate to achieve the purposes for which it was collected. Additionally, the information cannot be further processed for any purposes that is incompatible with the purpose for which it was originally collected.⁷²

On the federal level, the Federal Trade Commission (FTC) brought actions against two companies within a few days of each other for allegations that they violated Section 5 of the FTC Act by not implementing procedures for inventorying and deleting personal information after there was no longer a need to retain the information.⁷³

This hyper-focused approach by the CCPA raises signals that if there is no longer a need to keep the information around, businesses should delete it. After all, the more information the business has on file, the greater its potential liability if that information was the target of a breach or unauthorized access.

⁷¹ 11 CCR § 7101

⁷² Civil Code § 1798.100(c)

⁷³ Compl., In re Chegg, Inc., FTC File No. 202-3151 (Oct. 31, 2022); Compl., In re Drizly, LLC, FTC File No. 202-3185 (Oct. 24, 2022).

Section 16: Requirement 12 – Cybersecurity Requirements

The CCPA broadly requires the implementation of “reasonable” cybersecurity measures to safeguard consumer data and minimize the risk of data breaches.⁷⁴ In this section, we will discuss the data breach liability under the CCPA, the California Attorney General's reference to the Center for Internet Security (CIS) Controls for achieving reasonable security standards, and the overlap with the federal GLBA Safeguards Rule that dealers should consider maintaining.

California Attorney General's Reference to CIS Controls for Achieving Reasonable Security

While the CCPA doesn't clarify what it means by “reasonable” data protection and cybersecurity protocols, the California Attorney General's office has previously referenced the Center for Internet Security (CIS) Controls as a framework for achieving minimum “reasonable” security measures. In a February 2016 Data Breach Report, Kamala D. Harris, the then State Attorney General, and the California Department of Justice stated that the failure to implement the CIS Controls that apply to an organization's environment constitutes a lack of reasonable security. The CIS Controls provide a set of best practices that businesses can adopt to protect their networks and data from cyberthreats. By implementing the CIS Controls, dealerships can demonstrate their commitment to data security and compliance with the CCPA's reasonable security standards.

Data Breach Liability Under the CCPA

The CCPA holds businesses accountable for data breaches resulting from inadequate security measures. In the event of a data breach, affected consumers may have the right to file a lawsuit in a private right of action against the dealership seeking statutory damages ranging from \$100 to \$750 per consumer per incident, or actual damages, whichever is greater.⁷⁵ This potential liability highlights the importance of implementing robust cybersecurity measures to protect consumer data and meet the reasonable security standards required by the CCPA.

Overlap with the Federal GLBA Safeguards Rule

The Gramm-Leach-Bliley Act (GLBA) Safeguards Rule, recently revised by the FTC and, effective June 9, 2023, sets forth requirements for financial institutions (including dealerships) to protect the security, confidentiality, and integrity of customer information. Compliance with the specific requirements of the Safeguards Rule can help dealerships meet CCPA data protection requirements. For a comprehensive discussion of the revised

⁷⁴ 11 CCR §§ 7023(d)(4), 7101(a)

⁷⁵ Civil Code § 1798.150

Safeguards Rule, please refer to the CNCDA guide titled [Complying with the Revised FTC Safeguards Rule](#).

Transmitting Data in Response to Right to Know Requests

CCPA regulations require that dealers securely transmit data when responding to Right to Know requests and emphasized the importance of safeguarding consumers' personal information during the process.⁷⁶ Relying on traditional email communication to share this sensitive information is insufficient and may not meet the regulatory requirements to secure the information in transit. Specifically, Right to Know requests may contain highly sensitive data regarding a consumer's personal information, which necessitates heightened security measures. To comply with the CCPA and protect consumers' privacy, businesses should utilize a secure and encrypted portal for uploading and transmitting requested data. These portals should also include identity verification processes to ensure that only the authorized consumer can access their personal information.

⁷⁶ 11 CCR § 7024(f)

Section 17: Requirement 13 – Employee Training

CCPA regulations specifically require employee training to ensure that businesses maintain compliance and that their staff members are knowledgeable about the California privacy requirements.⁷⁷ Additionally, by investing in employee training and adopting best practices, dealers can promote a culture of privacy compliance, improve customer relations, and minimize the risk of non-compliance with the CCPA. It is also important to note that insufficient employee training would very likely be considered a negative factor by the California Privacy Protection Agency (Agency) when weighing potential enforcement actions against non-compliant businesses.

Identifying Applicable Personnel

According to the regulatory language, businesses should ensure that all individuals responsible for handling consumer inquiries about the business's privacy practices or compliance with the CCPA are informed of all the requirements of the CCPA and its accompanying regulations.⁷⁸ Due to the ambiguity of this language, dealerships should consider providing training to *all* consumer-facing employees and human resources personnel (meaning that service technicians probably do not need to take CCPA training if they do not regularly interface with customers). This approach ensures that staff members who interact with customers, job applicants, or employees are well-equipped to effectively address any CCPA-related questions or concerns (or at least know where to direct them) and prevent potential consumer or employee complaints.

Frequency of Training

While neither the law nor regulations specify how often employees should be trained on the CCPA, it is recommended that dealerships provide yearly training for all relevant staff members in order to keep employees updated on the latest privacy regulations and dealership practices. Additionally, new employees who will be responsible for handling consumer inquiries about privacy practices should receive training as part of their onboarding process to ensure that they are familiar with CCPA requirements from the outset of their employment.

⁷⁷ 11 CCR § 7100

⁷⁸ 11 CCR § 7100

Section 18: Requirement 14 – Disability & Foreign Language Requirements

Dealerships should also be mindful of the Web Content Accessibility Guidelines (WCAG) and foreign language requirements of the CCPA.

Web Content Accessibility Guidelines (WCAG)

CCPA regulations require that disclosures such as the privacy policy, Notice at Collection, cookie consent banners, and online consumer request portals meet compliance with WCAG 2.1 to ensure that web content is accessible to people with disabilities.⁷⁹ Adhering to WCAG 2.1 can also help dealerships minimize the risk of accessibility-related lawsuits such as those relating to the federal Americans with Disabilities Act (ADA). To meet WCAG 2.1 guidelines, dealers must optimize their websites for screen readers, offer alternative text for images, and ensure that navigation is user-friendly and accessible to a wide range of users. Dealers should conduct a thorough review of their websites and consult with web developers or accessibility experts to implement the necessary changes to achieve compliance.

Foreign Language Requirements

All disclosures under the CCPA must be provided in the languages in which the dealer ordinarily communicates with its consumers or for which it posts other signs or disclosures in a foreign language.⁸⁰ For example, if a dealer commonly negotiates in Spanish or has signs and other disclosures in Spanish, all CCPA-related disclosures must be offered in Spanish as well. Dealers must identify the languages in which the dealership ordinarily communicates with its customers and ensure that all CCPA-related materials are translated accurately and professionally into those languages.

⁷⁹ 11 CCR § 7003(b)(3)

⁸⁰ 11 CCR § 7003(b)(2)

Section 19: Enforcement & Penalties for Noncompliance

The CCPA imposes strict enforcement measures and penalties for non-compliance and dealers have been among one of the first targets and top priorities in enforcement sweeps announced by the California Attorney General (AG). A press release⁸¹ announcing the enforcement against a dealership and accompanying enforcement data have one common theme – the AG cares about the technical provisions of the CCPA and will heavily scrutinize the business’s existing practices. Prior to the press release, many thought the AG would just be looking for the more obvious low-hanging fruit. However, the AG cited the dealership for technical violations, such as the failure to have a designated toll-free number and a process for authorized agents to submit CCPA requests. The AG’s enforcement data revealed other common technical violations:

- Non-compliant CCPA service provider contracts.
- Failure to link to CCPA Notice at Collection in marketing emails.
- Failure to acknowledge and respond to requests within designated time limits.
- Missing a clear and easy-to-find “Do Not Sell My Personal Information” link (under the latest regulations, the link can now be titled “Your CA Privacy Choices”).
- Requiring that authorized agents provide notarized documentation.
- Requiring government-issued identification for exercising rights.

It is also worth noting that, on several occasions and most notably its complaint against *Sephora*,⁸² the AG has reinforced its position that a “sale” of information occurs even when there is simply an exchange of information for “valuable consideration” such as that provided in the context of analytics and retargeting services with companies like Meta and Google. As discussed earlier in [Section 5](#), since most dealerships deploy third-party tracking cookies for retargeting ads, this means that almost every dealership is “selling” or “sharing” information as those terms are defined under the CCPA. In short, the enforcement data highlights that a lackadaisical approach to CCPA compliance simply is not good enough. It is crucial for dealers to understand the potential consequences and take necessary steps to ensure compliance.

Monetary Penalties

Non-compliance with the CCPA can result in significant financial penalties to the business, ranging from \$2,500 per violation for non-intentional violations to \$7,500 per violation for intentional violations.⁸³ These penalties can be assessed on a per-consumer basis, which means the total amount can escalate rapidly.

⁸¹ *Attorney General Bonta Announces First-Year Enforcement Update on the California Consumer Privacy Act, Launches New Online Tool for Consumers to Notify Businesses of Potential Violations*, State of California Department of Justice, July 19, 2021, <https://oag.ca.gov/news/press-releases/attorney-general-bonta-announces-first-year-enforcement-update-california>

⁸² *People v. Sephora USA, Inc.*, <https://oag.ca.gov/system/files/attachments/press-docs/Complaint%20%288-23-22%20FINAL%29.pdf>

⁸³ Civil Code § 1798.199.55(a)(2)

Private Right of Action

The CCPA provides a limited private right of action for consumers in the event of certain data breaches allowing them to seek damages ranging from \$100 to \$750 per incident or actual damages, whichever is greater.⁸⁴ While the private right of action does not cover all CCPA violations, this has not deterred plaintiff lawyers from filing lawsuits (including class actions) based on the CCPA. Most of these lawsuits involve data breaches, inaccurate privacy policies, and notice at collection requirements. Accordingly, dealers may still face legal challenges and reputational damage even in the absence of direct enforcement action from the AG.

California Privacy Protection Agency (Agency)

The CCPA establishes the Agency as an enforcement authority with the power to issue fines against businesses for non-compliance⁸⁵ and allocated at least \$10 million from California's General Fund annually for its operation.⁸⁶ The Agency's funding structure, which relies on penalties levied against non-compliant businesses, creates an incentive for the Agency to actively and eagerly pursue enforcement actions to hold businesses accountable.

Data Breaches

The CCPA heightens the risks associated with data breaches as it grants consumers the right to sue businesses for damages resulting from unauthorized access, theft, or disclosure of their personal information. Ensuring that robust data security measures are in place is essential to minimize the risk of breaches and the associated legal, financial, and reputational consequences.

⁸⁴ Civil Code § 1798.150(a)(1)

⁸⁵ Civil Code §§ 1798.185(d), 1798.199.10(a)

⁸⁶ Proposition 24 Amends Consumer Privacy Laws. Initiative Statute, LEGISLATIVE ANALYST'S OFFICE, THE CALIFORNIA LEGISLATURE'S NONPARTISAN FISCAL AND POLICY ADVISOR (Nov. 3, 2020), <https://lao.ca.gov/BallotAnalysis/Proposition?number=24&year=2020>, accessed May 4, 2023.

Section 20: Automakers

No doubt dealers have seen some kind of communication sent from their automakers alerting them to the CCPA. Specifically, this notice comes in the form of an updated data sharing agreement that automakers have encouraged dealers to sign, but what does it all mean? Given that there are multiple versions of these data sharing agreements sent to dealers depending on their data collection practices, we cannot capture every single variation or clause within the agreements here, but we can speak to why the automakers are sending them to you. Dealers who require further clarification or advice should reach out to their in-house counsel or attorneys for more information.

Automaker as a Third Party

Under the definitions of the CCPA, automakers generally qualify as Third Parties. As noted earlier, Third Parties are those vendors who (a) collect consumers' personal information and (b) are *not* Service Providers. Because Service Providers are defined in the negative in the CCPA, i.e. what they are *not* allowed to do with the consumer's personal information that they collect, Third Parties are essentially vendors who perform these prohibited acts. Meaning, Third Parties can do any of the following things:

1. Sell or share the personal information;
2. Retain, use, or disclose the personal information for any purpose;
3. Retain, use, or disclose the personal information outside of their business relationship with the dealer; or
4. Combine the personal information it receives with any other information it collects from other vendors.

Automakers and Third-Party Contracts

The new regulations introduce a new requirement in that Third Parties must sign a contract with the dealer that has very specific requirements and prohibitions. Without this contract, the Third Party cannot collect, use, process, retain, sell, or share the personal information that the dealer has made available to the Third Party.⁸⁷

As discussed in a previous section, this contract between the dealer and automakers may contain language that does each of the following:⁸⁸

- Identifying the limited and specific purpose(s) for which the personal information is made available to the Third Party;
- Stating that the personal information is made available only for the limited and specific purpose(s) set forth within this contract;

⁸⁷ 11 CCR § 7052

⁸⁸ 11 CCR § 7053(a)

-
- Requiring the Third Party to comply with all applicable sections of the CCPA by providing the same level of privacy protection as required by the dealer;
 - Granting the dealer the right to take reasonable and appropriate steps to ensure that the Third Party uses it in a manner that is consistent with the dealer's obligations under the CCPA and its accompanying regulations;
 - Upon receiving written notice from the dealer, taking appropriate steps to stop and remediate unauthorized use of personal information made available to the Third Party; and
 - Notifying the dealer as soon as practicable after the Third Party determines that it can no longer meet its obligations under the CCPA or its accompanying regulations.

These clauses are probably included in the data processing agreement that was discussed earlier in this section. Dealers who require further clarification or advice should reach out to their in-house counsel or attorneys for more information.

Section 21: Privacy Management Software

Given the numerous and complex requirements of the CCPA and CPRA, dealers should seriously consider adopting privacy management software to help them navigate and maintain compliance with these regulations. Privacy management software can simplify the process of addressing regulatory requirements, reduce the risks of non-compliance, and save valuable time and resources for the dealer so they can rededicate those efforts to selling and servicing motor vehicles.

[ComplyAuto](#) is a leading choice in privacy management software among dealers and is currently licensed by the CNCDA and endorsed by the National Automobile Dealers Association (NADA), currently representing over 60% of dealerships in California and over 8,000 dealers across the country. By choosing [ComplyAuto](#), dealers benefit from a proven solution that automates the complexities of privacy compliance, including performing data mapping, building a systems inventory, creating a comprehensive privacy policy and Notice at Collection, installing a compliant and effective cookie consent banner, managing vendor contracts and addendums, and automating the many types of consumer privacy requests and navigating their requirements.

Questions

Please do not hesitate to contact ComplyAuto at info@complyauto.com if you have any questions about this compliance manual.

Appendix A – Sample Privacy Policy

IMPORTANT NOTE:

The following sample privacy policy is presented for educational purposes only. The privacy policy that a dealer uses must be unique to that dealer. Privacy policies vary widely depending on a dealer's data collection and retention practice, the types of vendors in which they work with, and the products and services they offer to their customers, employees, and job applicants. Please review the manual or contact our partners at ComplyAuto for more information.

Privacy Policy

Last Updated: April 28, 2023

Change language



California Notice at Collection

To view the categories of personal information we collect and the purposes for which the information is used, or to exercise your rights under the California Consumer Privacy Act (CCPA), click the button below.

[View Notice At Collection](#)

To view how we collect and use personal information as part of our online chat module, click the button below.

[View Chat Module Disclosure](#)

Introduction

[DEALERSHIP] ("Dealership" or "we" or "us") respects your privacy and the information that you have entrusted to us. This Privacy Policy describes our collection, use, and disclosure of the information we may collect from you whenever you visit the Dealership's physical location(s) or website(s) (hereinafter a "Site" and collectively the "Sites"), or otherwise access any of our other products, services, and content (hereinafter "Services"). This Privacy Policy applies to all visitors and customers of our Sites, including those consumers and/or customers who apply for and/or receive financing for personal, family, or household purposes. If you become an inactive customer, or if we close or suspend your account, we will continue to adhere to the Privacy Policy in place when we collected your personal information.

as long as we retain it in our databases. We may delete any or all of your information at any time without notice to you or for any reason or no reason unless we are otherwise required by law to retain it. You may have other privacy protections under state laws and we will comply with any applicable state laws when we disclose information about you.

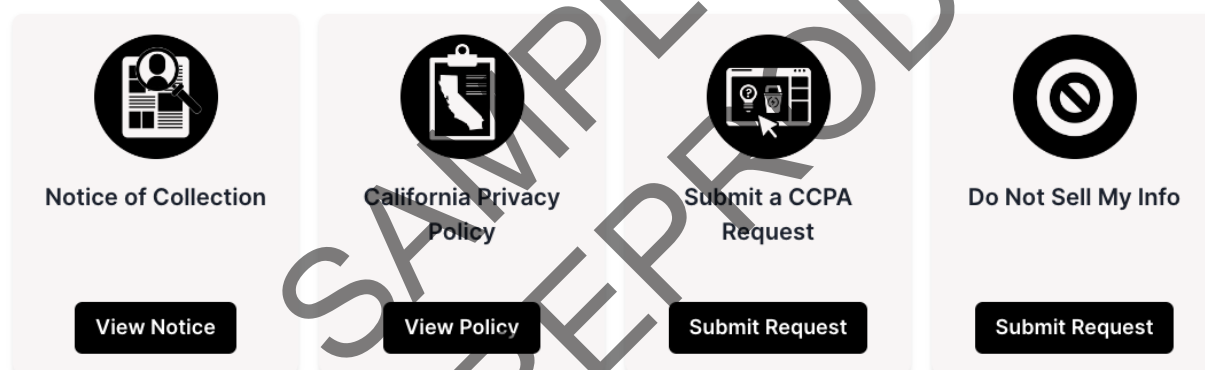
Sections

This Privacy Policy consists of the following sections.

Section 1 - California Consumer Privacy Act Disclosures

Section 2 - Other Important Privacy Disclosures

Section 1 - California Consumer Privacy Act Disclosures



Notice at Collection

The purpose of this Notice at Collection is to provide consumers with information about the categories of personal information that our dealerships collect about them and the purposes for which the personal information will be used.

We collect the following categories of “personal information”, as defined in the CCPA, relating to California residents and businesses:

- **Audio / Video / Visual / Electronic** such as photographs, recorded calls, voicemails, and online & electronic communications, such as those made via a live or automated online chat module.
- **Biometric** such as fingerprints and facial recognition.
- **Commercial** such as vehicles, products, services, and repairs purchased, obtained, or considered; personal property records (e.g., vehicle titles and registration cards); or other purchasing or consuming histories or tendencies.
- **Customer Records** such as digital and electronic signatures, telephone numbers, insurance policy numbers, credit and debit card numbers, financial and credit-related information, physical characteristics and descriptions (e.g., government identification), bank account numbers, and medical and health insurance information (in the context of employment).
- **Education** such as diplomas and transcripts for student rebate eligibility.
- **Geolocation** such as tracking and user-enabled location identification.
- **Identifiers** such as real name, postal address, IP address, email address, SSN, driver's license number, passport number, cookies, pixel tags, and similar identifiers.

- **Inferences** to create a profile about you reflecting your product or vehicle preferences, purchasing tendencies and behaviors.
- **Internet Activity** such as interactions with our websites, applications, and advertisements.
- **Professional/Employment** such as job title, occupation, company or business name, and employment history information.
- **Protected Classes** under state or federal law, such as gender, age, and veteran status.

We use the categories of personal information listed above for one or more of the following “business purposes” listed in the CCPA:

- **Advertising & Marketing** to send advertisements and marketing material via physical and electronic mail relating to product specials and other promotional events or offers, perform marketing research and data analytics, and perform similar activities.
- **Claims & Benefits Administration** to process claims, administer benefits, and conduct employee drug tests in accordance with applicable laws.
- **Contextual and Behavioral Targeting** to provide contextual customization of ads shown as part of an interaction with our website or application, such as through the use of “first-party” or “session” cookies.
- **Counting Ad Impressions & Website Interactions** to audit interactions with our websites, applications, advertisements, count ad impressions to unique visitors, verify position and quality of ad impressions, and perform similar activities.
- **Customer Service** to provide customer service, maintain and service products and accounts, provide training for quality assurance purposes, and perform similar activities.
- **Defending Against Claims & Litigation** to defend against or respond to potential or actual claims and litigation, including, but not limited to, those against the manufacturer of a particular vehicle we've sold.
- **Determining Employment Eligibility** to determine eligibility for employment, verify references and employment history, and conduct background checks.
- **Employee Engagement & Emergency Contact Communications** to communicate and engage with employees across the organization, enhance company morale by acknowledging significant events (e.g., birthdays, work anniversaries, etc.) and reaching out to emergency contacts listed for employees.
- **Employee Onboarding** to conduct employee onboarding.
- **Employee Productivity** to ensure employee productivity and adherence to company policies.
- **Fraud Prevention** to help ensure security and integrity, such as necessary to detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, and to prosecute those responsible for that activity.
- **Human Resources Support & Services** to provide employees with human resources management services and employee data maintenance and support services.
- **Internal Audits & Investigations** to conduct internal audits and investigate complaints, grievances, and suspected violations of internal policies.
- **Monitoring Driving Records** to monitor employee driving records as required or allowed by state and federal law.
- **Performance Evaluations & Customer Satisfaction** to evaluate employee performance during the service and/or sales process and monitor customer satisfaction.
- **Preventing Unauthorized Access** to prevent unauthorized access to or use of company property, including information systems, electronic devices, network, and data.
- **Processing Transactions** to process or fulfill orders and transactions, verify customer information, process payments, confirm eligibility for manufacturer rebates, and perform similar activities.
- **Providing Financing** to provide financing in connection with a vehicle purchase, lease, or related products or services.
- **Public Health and Safety** to conduct screening or temperature checks for COVID-19 symptoms or similar screening activities related to public health and safety.

In the context of employment, we also use the categories of personal information listed above for one or more of the following business purposes:

- **Claims & Benefits Administration** to process claims, administer benefits, and conduct employee drug tests in accordance with applicable laws.
- **Determining Employment Eligibility** to determine eligibility for employment, verify references and employment history, and conduct background checks.
- **Employee Engagement & Emergency Contact Communications** to communicate and engage with employees across the organization, enhance company morale by acknowledging significant events (e.g., birthdays, work anniversaries, etc.) and reaching out to emergency contacts listed for employees.
- **Employee Onboarding** to conduct employee onboarding.
- **Employee Productivity** to ensure employee productivity and adherence to company policies.
- **Human Resources Support & Services** to provide employees with human resources management services and employee data maintenance and support services.
- **Internal Audits & Investigations** to conduct internal audits and investigate complaints, grievances, and suspected violations of internal policies.
- **Monitoring Driving Records** to monitor employee driving records as required or allowed by state and federal law.
- **Performance Evaluations & Customer Satisfaction** to evaluate employee performance during the service and/or sales process and monitor customer satisfaction.
- **Preventing Unauthorized Access** to prevent unauthorized access to or use of company property, including information systems, electronic devices, network, and data.
- **Public Health and Safety** to conduct screening or temperature checks for COVID-19 symptoms or similar screening activities related to public health and safety.

We collect the following categories of “sensitive personal information”, as defined in the CCPA, relating to California residents:

- **Biometric Data for Identification Purposes** such as fingerprints and facial recognition used to identify you for the purposes of identity verification and fraud and theft prevention.
- **Contents of Communications** such as a consumer’s mail, email, and text messages unless the business is the intended recipient of the communication.
- **Genetic Data** such as family medical history in the context of employment.
- **Government-Issued ID Numbers** such as social security, driver’s license, state identification, or passport numbers.
- **Health Information** such as necessary to administer employee health benefits, make special accommodations, and respond to work-related illnesses and injuries.
- **Online Account or Credit Card Info Combined with a Security/Access Code** such as account login information, credit or debit card numbers, or financial account information that is combined with a security or access code.
- **Precise Geolocation Data** such as tracking and online user-enabled location identification that is accurate within a radius of 1,850 feet.
- **Race, Ethnicity, Religion, Philosophical Beliefs, or Union Membership** which may be collected in the context of employment.

Record Retention Notice

We will store your personal information for as long as reasonably necessary for the purposes in which it was collected. In general, the criteria used to determine the length of time that we will retain this information is based on California record retention rules and guidelines, which can be found [here](#). However, note that some of your personal information may need to be retained for longer periods and may not have a set retention period because it is needed for an ongoing business or legal purpose.

Your California Privacy Choices

To opt out of the sale or sharing of your personal information; or to limit the use of your sensitive personal information, [click here](#).

California Privacy Policy

The purpose of this California Privacy Policy is to provide consumers with a comprehensive description of our dealership's online and offline practices regarding the collecting, use, disclosure, and sale of personal information and of the rights of consumers regarding their personal information under the CCPA.

The tables below describe how we collect, use, and disclose California consumers' personal information based on definitions laid out in the CCPA. Please note that because the categories of personal information collected and shared largely depends on how a consumer has interacted with our dealership, not all of the items listed in the tables below will be relevant to you. For example, we generally only collect veteran status when a consumer qualifies for a military rebate. Similarly, certain pieces of information, such as health and medical information, are only collected in the course of administering employment benefits and claims, but are not collected from customers.

Categories of Personal Information We Collect

Categories of Personal Information Collected	Categories of Sources from which the Personal Information is Collected	Business or Commercial Purposes for which the Personal Information was Collected or Sold
Audio / Video / Visual / Electronic such as photographs, recorded calls, voicemails, and online & electronic communications, such as those made via a live or automated online chat module.	Advertising Networks & Agencies such as digital advertising companies and other marketing firms. Captive Finance Companies and wholly-owned subsidiaries of automakers that offer loans, lease programs, and other financial services to our customers. Cell Phone Carriers otherwise referred to as wireless service providers, wireless carriers, cellular companies, or mobile network carriers.	Advertising & Marketing to send advertisements and marketing material via physical and electronic mail relating to product specials and other promotional events or offers, perform marketing research and data analytics, and perform similar activities. Claims & Benefits Administration to process claims, administer benefits, and conduct employee drug tests in accordance with applicable laws.
Biometrics such as fingerprints and facial recognition.	Credit Reporting Agencies such as Experian, Transunion and Equifax that gather account information from various creditors and provide that information to dealers in connection with an application for credit.	Contextual and Behavioral Targeting to provide contextual customization of ads shown as part of an interaction with our website or application, such as through the use of "first-party" or "session" cookies.
Commercial such as vehicles, products, services, and repairs purchased, obtained or considered, personal property records (e.g., vehicle titles and registration cards); or other purchasing or consuming histories or tendencies.	Data Brokers & Analytics Providers such as equity mining, data mining, call tracking, and sales prospecting tools.	Counting Ad Impressions & Website Interactions to audit interactions with our websites, applications, or advertisements, count ad impressions to unique visitors, verify position and quality of ad impressions, and perform similar activities.
Customer Records such as digital and electronic signatures, telephone numbers, insurance policy numbers, credit and debit card numbers, financial and credit-related information, physical characteristics and descriptions (e.g., government identification), bank account numbers, and medical and health insurance information (in the context of employment).	Directly from Consumers through our website forms and via in-person applications, forms and contracts.	Customer Service to provide customer service, maintain and

Education such as diplomas and transcripts for student rebate eligibility.	Government Entities such as the Department of Motor Vehicles (DMV) and various other state and federal agencies.	service products and accounts, provide training for quality assurance purposes, and perform similar activities.
Geolocation such as tracking ad user-enabled location identification.	Insurance Companies that provide us with information relating to vehicle collisions, auto accidents, and other claims.	Defending Against Claims & Litigation to defend against potential or actual claims and litigation, including, but not limited to, those against the manufacturer of a particular vehicle we've sold.
Identifiers such as real name, postal address, IP address, email address, SSN, driver's license number, passport number, cookies, pixel tags, and similar identifiers.	Internet Service Providers that provide services for accessing, using, or participating in the internet.	Determining Employment Eligibility to determine eligibility for employment, verify references and employment history, and conduct background checks.
Inferences to create a profile about you reflecting your product or vehicle preferences, purchasing tendencies and behaviors.	Job Boards & Screening Companies such as background check companies and services that allow job seekers to submit resumes and apply to us directly.	Employee Engagement & Emergency Contact Communications to communicate and engage with employees across the organization, enhance company morale by acknowledging significant events (e.g., birthdays, work anniversaries, etc.) and reaching out to emergency contacts listed for employees.
Internet Activity such as interactions with our websites, applications, and advertisements.	Online Lead Providers and third party websites that collect and share data relating to consumers whose product preferences or inquiries align with the offerings of our dealership.	Employee Onboarding to conduct employee onboarding.
Professional/Employment such as job title, occupation, company or business name, and employment history information.	Social Media Networks such as Facebook, Instagram, and other platforms used to run various advertising campaigns.	

Protected Classes under state or federal law, such as gender, age, and veteran status.	Towing Companies that transport customer vehicles to the dealer's service department. Vehicle Manufacturers for which we are franchised to sell new motor vehicles. Vehicle Subscription Services that partner with dealerships to deliver vehicles to customers that subscribe to their short-term or month-to-month vehicle programs.	Employee Productivity to ensure employee productivity and adherence to company policies. Fraud Prevention to help ensure security and integrity, such as necessary to detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, and to prosecute those responsible for that activity. Human Resources Support & Services to provide employees with human resources management services and employee data maintenance and support services. Internal Audits & Investigations to conduct internal audits and investigate complaints, grievances, and suspected violations of internal policies. Monitoring Driving Records to monitor employee driving records as required or allowed by state and federal law. Performance Evaluations & Customer Satisfaction to evaluate employee performance during the service and/or sales process and monitor customer satisfaction. Preventing Unauthorized Access to prevent unauthorized access to or use of company property, including information systems, electronic devices, network, and data. Processing Transactions to processor fulfill orders and transactions, verify customer information, process payments, confirm eligibility for manufacturer rebates, and perform similar activities. Providing Financing to provide financing in connection with a vehicle purchase, lease or related products or services.
--	---	--

Public Health and Safety to conduct screening or temperature checks for COVID-19 symptoms or similar screening activities related to public health and safety.

Disclosure of Personal Information to Third Parties

Categories of Personal Information Disclosed for a Business Purpose or Sold to Third Parties	Categories of Third Parties to Whom the Information was Disclosed or Sold
Audio / Video / Visual / Electronic such as photographs, recorded calls, voicemails, and online & electronic communications, such as those	Attorneys & Law Firms, Social Media Networks, Software Vendors
Biometric such as fingerprints and facial recognition.	Attorneys & Law Firms, Records Management Companies, Software Vendors
Commercial such as vehicles, products, services, and repairs purchased, obtained or considered; personal property records (e.g., vehicle titles and registration cards); or other purchasing or consuming histories or tendencies.	Advertising Networks & Marketing Agencies, Attorneys & Law Firms, Auctions & Wholesalers, Auditors & Consultants, Car Rental Companies, Chat Modules, Check Guarantee Companies, Data Brokers & Analytics Providers, Debt Collection Agencies & Repossession Companies, Digital Retailers & eCommerce Platforms, F&I Product Providers & Administrators, Financial Institutions, Government Entities, Insurance Brokers (non-health related), Lien Sale Companies, Professional Service Companies, Records Management Companies, Repair & Sublet Facilities, Reputation Management Companies, Social Media Networks, Software Vendors, Transportation Companies, Vehicle Manufacturers, Website and Hosting Providers
Customer Records such as digital and electronic signatures, telephone numbers, insurance policy numbers, credit and debit card numbers, financial and credit-related information, physical characteristics and descriptions (e.g., government identification), bank account numbers, and medical and health insurance information (in the context of employment).	Advertising Networks & Marketing Agencies, Attorneys & Law Firms, Auctions & Wholesalers, Auditors & Consultants, Car Rental Companies, Chat Modules, Check Guarantee Companies, Claims & Benefits Administrators, Credit Reporting Agencies (CRAs), Data Brokers & Analytics Providers, Debt Collection Agencies & Repossession Companies, Digital Retailers & eCommerce Platforms, Employee Screening & Background Check Companies, F&I Product Providers & Administrators, Financial Institutions, Government Entities, Insurance Brokers (non-health related), Payment Processors & Gateways, Professional Service Companies, Records Management Companies, Repair & Sublet Facilities, Reputation Management Companies, Rideshare Companies, Social Media Networks, Software Vendors, Towing Companies, Transportation Companies, Vehicle Manufacturers, Website and Hosting Providers
Education such as diplomas and transcripts for student rebate eligibility.	Attorneys & Law Firms, Auditors & Consultants, Debt Collection Agencies & Repossession Companies, Financial Institutions, Records Management Companies, Software Vendors, Vehicle Manufacturers, Website and

	Hosting Providers
Geolocation such as tracking and user-enabled location identification.	Advertising Networks & Marketing Agencies, Attorneys & Law Firms, Chat Modules, Digital Retailers & eCommerce Platforms, Social Media Networks, Software Vendors, Vehicle Manufacturers, Website and Hosting Providers
Identifiers such as real name, postal address, IP address, email address, SSN, driver's license number, passport number, cookies, pixel tags, and similar identifiers.	Advertising Networks & Marketing Agencies, Attorneys & Law Firms, Auctions & Wholesalers, Auditors & Consultants, Car Rental Companies, Chat Modules, Check Guarantee Companies, Claims & Benefits Administrators, Credit Reporting Agencies (CRAs), Data Brokers & Analytics Providers, Debt Collection Agencies & Repossession Companies, Digital Retailers & eCommerce Platforms, Employee Screening & Background Check Companies, F&I Product Providers & Administrators, Financial Institutions, Government Entities, Insurance Brokers (non-health related), Lien Sale Companies, Payment Processors & Gateways, Professional Service Companies, Records Management Companies, Repair & Sublet Facilities, Reputation Management Companies, Rideshare Companies, Social Media Networks, Software Vendors, Tow Companies, Transportation Companies, Uniform & Apparel Companies, Vehicle Manufacturers, Website and Hosting Providers
Inferences to create a profile about you reflecting your product or vehicle preferences, purchasing tendencies and behaviors.	Advertising Networks & Marketing Agencies, Data Brokers & Analytics Providers, Digital Retailers & eCommerce Platforms, Social Media Networks, Software Vendors, Vehicle Manufacturers, Website and Hosting Providers
Internet Activity such as interactions with our websites, applications, and advertisements.	Advertising Networks & Marketing Agencies, Attorneys & Law Firms, Chat Modules, Data Brokers & Analytics Providers, Digital Retailers & eCommerce Platforms, Reputation Management Companies, Social Media Networks, Software Vendors, Vehicle Manufacturers, Website and Hosting Providers
Professional/Employment such as job title, occupation, company or business name, and employment history information.	Attorneys & Law Firms, Auditors & Consultants, Claims & Benefits Administrators, Credit Reporting Agencies (CRAs), Data Brokers & Analytics Providers, Debt Collection Agencies & Repossession Companies, Digital Retailers & eCommerce Platforms, Employee Screening & Background Check Companies, Financial Institutions, Government Entities, Insurance Brokers (non-health related), Records Management Companies, Social Media Networks, Software Vendors, Uniform & Apparel Companies, Website and Hosting Providers

Protected Classes under state or federal law, such as gender, age, and veteran status.	Attorneys & Law Firms, Auditors & Consultants, Car Rental Companies, Check Guarantee Companies, Claims & Benefits Administrators, Credit Reporting Agencies(CRAs), Data Brokers & Analytics Providers, Debt Collection Agencies & Repossession Companies, Digital Retailers & eCommerce Platforms, Employee Screening & Background Check Companies, Financial Institutions, Government Entities, Insurance Brokers (non-health related), Records Management Companies, Social Media Networks, Software Vendors, Vehicle Manufacturers, Website and Hosting Providers
--	---

Your Rights Under the CCPA

1. Right to Know About Personal Information Collected, Disclosed, or Sold

Under the CCPA, you have a right to request that we disclose the categories of personal information we have collected, used, disclosed, and sold. We call this a “categories” request. You also have the right to request that we disclose the specific pieces of personal information that we have collected about you, which we call a “specific pieces” request. These are referred to collectively as “Right to Know” requests under the CCPA.

2. Right to Request Deletion of Personal Information

You also have a right to delete the personal information we’ve collected about you. The “Right to Delete” is subject to several legal exceptions, such as when we are required by another state or federal law to retain your information.

3. Right to Opt-Out of the Sale or Sharing of Information

The CCPA provides consumers with the right to opt-out of the sale of their personal information and sharing of their personal information for cross-context behavioral advertising. The CCPA defines a “sale” as disclosing or making available to a third-party personal information in exchange for monetary or other valuable consideration. Cross-context behavioral advertising is defined as the targeting of advertising to a consumer based on the consumer’s personal information obtained from the consumer’s activity across businesses, distinctly-branded websites, applications, or services with which the consumer does not intentionally interact.

While we do not sell personal information for monetary value, we may disclose personal information to third parties, such as vehicle manufacturers, in such a way that may be considered a “sale” of personal information under the CCPA. We also share information with third-party advertising companies for cross-context behavioral advertising to identify and present advertisements tailored to your behavior (e.g., retargeting ads). To direct us to stop the sale or sharing of your personal information, [click here](#) to submit a request using our interactive web form.

We do not sell or share personal information of minors who we know are under 16 years of age.

4. Right to Non-Discrimination for the Exercise of Your CCPA Rights

You have a right not to receive discriminatory treatment for the exercise of the privacy rights conferred by the CCPA.

5. Right to Correct Inaccurate Personal Information

You have a right to correct any inaccurate personal information that we store on you.

6. Right to Limit the Use & Disclosure of Sensitive Personal Information

Under the CCPA, you have the right to limit the use and disclosure of your sensitive personal information for the purpose of inferring characteristics about you. Under California law, “sensitive personal information” includes, but is not limited to, your precise geolocation data, ethnicity, or social security, government-issued identification, bank account, or credit card number.

We may use and share certain categories of your sensitive information, such as geolocation data collected on our website, to infer characteristics about you. To direct us to stop the use and disclosure of your sensitive personal information, [click here](#) to submit a request using our interactive web form.

Verification of Right to Know, Correction and Deletion Requests

To protect against fraud, identity theft, and the unauthorized disclosure or deletion of personal information, we require that consumers submitting requests under the CCPA first verify their identity. This may include a combination of SMS (text message) verification, email verification, and one or more questions regarding the consumer's particular interaction or transaction with our dealership. If the consumer fails to verify their request via these methods, or the information provided by the consumer otherwise does not match our existing records, we will deny the request.

How to Submit a CCPA Request

To submit a Right to Know, Correct, Delete, Opt-Out, or Limit request, [click here](#) to access our online consumer request portal, or call our toll-free number at [DEALER PHONE NUMBER].

Authorized Agents

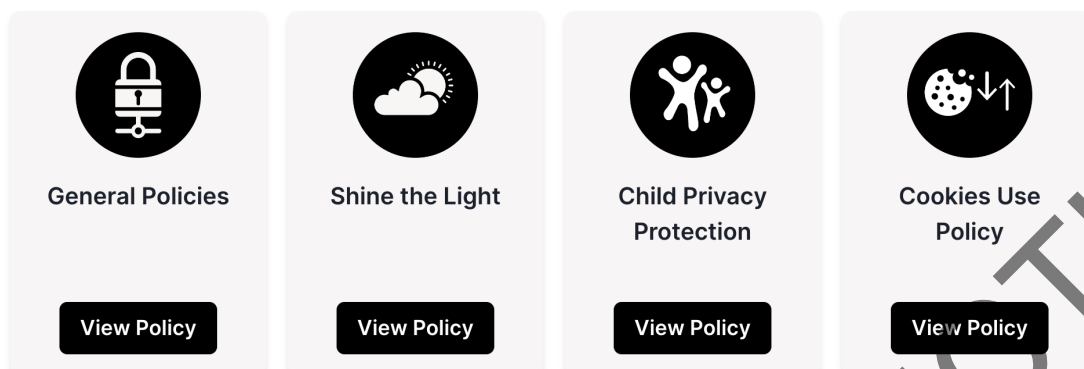
A consumer may designate an authorized agent to make a request under the CCPA on the consumer's behalf. If a consumer wishes to authorize another person to act as an authorized agent on the consumer's behalf, the consumer must provide the authorized agent permission to do so. An authorized agent can submit a CCPA request on behalf of a California resident by [clicking here](#).

To help prevent fraudulent requests, we reserve the right to deny a request from an agent that does not submit proof that he or she has been authorized by the consumer to act on the consumer's behalf. As proof that the agent has been duly authorized by the consumer to submit a CCPA request, the agent will be required to upload either (1) power of attorney signed by the consumer, or (2) other signed permission from the consumer. Pursuant to California Probate Code Sections 4300 to 4310, if an agent provides power of attorney signed by the consumer ("principal") that purports to give the agent authorization to submit the request on the principal's behalf, we may require that the agent provide information reasonably necessary or appropriate to identify the agent and principal and to facilitate the request. This includes, but is not limited to, identification of the agent and principal and the current and permanent residence addresses of the principal. If the agent provides some other signed permission from the consumer, we may require that the consumer (1) verify their identity directly with us through a combination of SMS (text message) verification, email verification, and one or more questions regarding the consumer's particular interaction or transaction with our dealership and (2) confirm that he or she provided the authorized agent permission to submit the request.

Contact Us

For questions or concerns about our California Privacy Policy, please contact us by email at [DEALER EMAIL] or by phone at [DEALER PHONE NUMBER].

Section 2 - Other Important Privacy Disclosures



Consent and Notification of Revisions

By accessing or using our Sites and/or Services, you consent to this Privacy Policy. If you do not agree with this Privacy Policy, please do not access or use the Site(s) or Services. We may periodically modify or update our Privacy Policy with or without notice to you by posting the most updated version on this page. Please see the "Revision Date" at the top of this document to see when the Privacy Policy was last changed. We will update the "Revision Date" in the privacy policy to notify you of any substantive changes to the way we collect and use information. We encourage you to periodically review this Privacy Policy to obtain the most up-to-date information on how we are handling your personal information. If you do not agree to changes to this Privacy Policy, you must stop using the Sites after the last revision date of such changes.

Collection of Anonymous Information

We also collect anonymous, aggregate information from all visitors to our Sites. The anonymous information we collect from your visit is never linked to any of your personal information until you voluntarily submit that personal information. If not, that anonymous information is used only in the aggregate to generate statistical reports about the use of our Sites. We may provide this anonymous information in aggregate form to other parties or use it for our own insights for marketing purposes. This anonymous or aggregate information is not linked to any personal information and our ability to use this information is not restricted in any way.

How We Respond To Do-Not-Track Signals & Global Privacy Controls

A "do-not-track" signal is a privacy preference feature in some web browsers that tells a website that a user does not want their online activity to be tracked. We currently support Global Privacy Control (GPC), a specification designed to allow internet users to notify businesses of their privacy preferences, such as whether or not they want to be tracked or have their personal information sold or shared with third parties for targeted advertising. It consists of a setting or extension in the user's browser or mobile device and acts as a mechanism that our websites can use to honor your privacy settings. GPC is available for an increasing number of browsers and browser extensions, [click here](#) to view the options. If you want to use GPC, you can download and enable it via a participating browser or browser extension. More information about downloading GPC can be found by [clicking here](#). If your browser or device has enabled GPC, it will override your preferences selected in the cookie banner or privacy settings on this Site.

Third-party Links

This Privacy Policy applies only to our Sites and Services, and information collected for us or by us through various features and online offerings on our Sites. Our Sites contain links to other third-party sites, and our Privacy Policy

does not apply to any third-party site or service linked to our Sites or recommended or referred by our Sites or by our staff. We are not responsible for the website, privacy practices or content of any third-party. If you have any questions about how these other sites use your information, you should review their policies and contact them directly.

Security

We implement reasonable security measures to ensure the security of your personal information. However, no data transmissions over the Internet can be guaranteed to be 100% secure by nature. Consequently, we 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. We may attempt to notify you electronically of any security system breach so that you can take appropriate 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 or send an email to you at the email address you provided. You may have a legal right to receive notice of a security breach in writing depending on where you live.

While we use encryption to protect online information, we also make all reasonable efforts to secure and protect your information offline. All of our customers' information is restricted in our offices and only employees who need the information to perform a specific job function are granted access to this information. The services that store your personal information are housed in a secure environment.

Business Transfers and Related Activities

We may share or transfer your information in the course of any direct or indirect reorganization process such as, but not limited to, mergers, acquisitions, divestitures, bankruptcies, and sales of all or a part of our assets. Your information may be shared as a result of such a transaction and/or during the assessment process pending transfer. In the event your information is transferred due to one of these events, know that your information would remain subject to this Privacy Policy or a privacy policy that protects your privacy to an equal degree as this Privacy Policy.

Chat Modules

We may collect certain categories of personal information from you when you use our interactive chat module. In addition to the information you may enter into the chat box or live chat feature, the categories of personal information include, but are not limited to, name, phone number, email, mailing address, and other identifiers you may provide. Additionally, we may also store any transcripts from such conversations and link those transcripts with your personal information. We may also collect information from you to perform data analytics and thereby enhance your experience and help improve the functionality of our tools and digital advertising in an effort to present to you only relevant products and services. Such Information includes, but is not limited to, geolocation, IP address, pixel tags, browsing history, viewing behavior, clicks, online activity, and other analytics. By interacting with the chat module, you understand and agree that we may use this data to communicate with you about our products and services. You also consent to our collection and analysis of all personal information provided as part of the chat module and understand that we utilize a vendor to process, analyze, and store the content of the chat on our behalf. By using the chat module, you are consenting to us disclosing and sharing with the chat module vendor any personal information you provide.

Your California Privacy Rights

California Civil Code Section 1798.83 permits visitors to our Sites and users of our Services who are California residents to request, once a year, certain information regarding our disclosure of personal information to third parties for their direct marketing purposes. To make a request, please send us an email at hao@privacy.com and include "Shine the Light Request" in the subject line.

Children Under 13 Years of Age

Our Sites and Services are not intended for children under thirteen (13) years of age. Dealership does not knowingly collect or use any personal information from children under thirteen (13) years of age, and does not knowingly

provide any personal information to any third party for any purpose whatsoever from visitors younger than thirteen (13) years old. If you are under thirteen (13) years old, please do not provide any information on our Sites or through our Services.

Use of Cookies & Similar Technologies

We use cookies and other similar technologies (e.g. web beacons, pixels, or local storage) to deliver content specific to your interests, track your website activity, help our Sites remember you, enhance your online experience with us, and provide you with information you're most likely to need. Cookies are small pieces of text used to store information on web browsers between visits. Cookies and any technology that serves a similar purpose as a cookie in the context of tracking, identifying, or building consumer profiles are included in our use of the term "cookie" for the purpose of this Privacy Policy. We, our service providers, or third-party advertising companies may use "first-party cookies" or "third-party cookies" as described below.

First-Party Cookies.

Many first-party cookies are necessary to facilitate essential website functions and enable you to navigate our Sites and use its features, such as remembering a consumer's shopping cart or chat session across pages or multiple visits. Also, first-party cookies are used to improve the functionality of the Site (such as tracking errors) and may be used to improve the ability to market or advertise to our consumers strictly on our own Sites, such as building consumer interest profiles to improve the recommended products consumers see on our own Sites. By default, our Sites do not support an inherent mechanism to allow users to opt-out of these first-party cookies.

Third-Party Cookies.

Third-party cookies refer to any cookie that shares or enables the sharing of information to an entity other than our own Sites. For example, some cookies used with third-party analytics providers will use a first-party domain but still share the collected information with the third-party provider. Our users can opt-out of certain third-party cookies by making the appropriate selection on our cookie banner that appears upon first visiting our Sites, using a browser or plug-in that supports Global Privacy Control (GPC), by submitting an opt-out request (see our Privacy Policy for more info), or as otherwise described in this Privacy Policy. We allow users to opt-out of the following types of third-party cookies:

- Cookies used to track consumers in order to serve ads to the consumer on other websites (e.g. retargeting ads that might appear on a search engine or social media that redirect you to our Sites).
- Cookies used to build consumer profiles to improve the overall ability to advertise to an individual or group of consumers across multiple Sites.
- Cookies used to track individual consumers to improve the ads they are served from a variety of advertisers (which may include the Dealership).

For some third-party cookies, our Sites do not offer an inherent mechanism for users to opt-out. This includes the following types of third-party cookies:

- Cookies used by our service providers or third-party advertising companies to perform an essential function solely on our own Sites. For example, they may use a cookie to remember a consumer's chat session across pages or visits so that the customer service representative responding to the chat is aware of the previous questions asked by the specific consumer.
- Cookies used by our service providers to perform analytics solely for our own Sites.

Some web browsers offer settings that allow you to choose whether cookies are set by the websites that you visit. These Controls vary by browser, but may allow you to disable all cookies, disable cookies for individual websites, or notify you whenever a cookie is set. Please note that if you disable cookies, you may still use our website, but your ability to use some features or areas of the Site may be limited. Our Sites may use products, such as Google Analytics, to measure how you interact with our Sites and to improve your user experience. For more information on Google Analytics, its 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>. For Google's privacy policy and instructions on opting-out of Google Analytics, please visit <https://tools.google.com/dlpage/gaoptout>. The Network Advertising Initiative also offers a means to opt-out of a number of advertising cookies. To learn more,

please visit www.networkadvertising.org. Note that opting-out does not mean you will no longer receive online advertising. It means that the company or companies from which you opted-out will no longer deliver ads tailored to your preferences and usage patterns.

Note that this site's cookie banner and privacy settings will only opt you out of the future tracking and sharing by cookies that are deployed by our Sites. In order to manage the information sharing and advertising cookies not deployed by our Sites (e.g., other third-party companies' cookies that are already tracking you), you may want to consider using one of the consumer choice tools created under self-regulation programs, such as the US-based <https://optout.aboutads.info/?c=2&lang=EN> choices page.

Dispute Resolution and Arbitration Agreement

Except where 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 Privacy Policy or any part of it (hereinafter "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) calendar days in which to respond to or settle the Dispute. Notice shall be sent to us at ATTN: [DEALER ADDRESS] or to you at the address or email we have on file for you.

Both you and the 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 ANY 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. 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 Privacy Policy, including any claims that all or any part of this Privacy Policy is void or voidable.

Other Arbitration Agreements

In the event of a conflict between this arbitration agreement 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 (hereinafter "Other Arbitration Agreement"), the terms of the Other Arbitration Agreement shall govern and prevail in each instance.

Venue And Choice Of Law

This Privacy Policy has been made in, and shall be construed in accordance with the laws 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 that state and you agree and submit to the exercise of personal jurisdiction of such courts for the purpose of litigating any such claim or action.

Appendix B – Compliance Checklist

IMPORTANT NOTE: This checklist provides general guidance on what dealerships need to have in place to fulfill the CPRA. Each of these items require a depth of knowledge and specific functionality that is not reflected here. For example, a “deletion request” needs to be verified and properly authenticated with three points of identification by the consumer before it can be properly processed and a “privacy policy” must have very specific disclosures. Please review the manual or contact our partners at [ComplyAuto](#) for more information.

Dealer Website		
#	Action	Notes
1	Cookie Consent Banner	Loading tracking or cross-contextual cookies on a Consumer’s device is considered a “sale” and therefore requires the Consumer’s consent prior to firing.
2a	Conspicuously place two specific links on the website AND at the header or footer	1. Link: <u>“Do Not Share or Sell My Personal Information,”</u> AND 2. Link: <u>“Limit the Use of My Sensitive Personal Information”</u>
OR		
2b	Conspicuously place link and opt-out icon adjacent to link at header or footer	1. Link: <u>“Your Privacy Choices”</u> AND 2. The following icon: 
3	California Privacy Policy	The privacy policy must have very specific disclosures as required by the CCPA as covered in <i>Section 8</i> .
4	Notice at Collection	The Notice at Collection provides the consumer, employee or job applicant with timely notice, at or before the time of collection, about the categories of personal information to be collected from them and the purposes for which the personal information is collected or used, and whether it is sold or shared.
5	Opt-Out Preference Signals	The dealer must enable a mechanism on the website to honor standardized opt-out preference signals, including Global Privacy Control (GPC).

Consumer Rights		
#	Action	Notes
1	Respond to a “Right to Know” request - Categories	The dealer must put two or more mechanisms in place to respond to these types of requests it receives both online and in-person. This means responding to the consumer, employee or job applicant within the statutory deadlines. This mechanism must properly notify downstream Service Providers, Contractors, and Third Parties if applicable.
2	Respond to a “Right to Know” request - Specific Pieces	The dealer must put two or more mechanisms in place to respond to these types of requests it receives both online and in-person. This means responding to the consumer, employee or job applicant within the statutory deadlines. This mechanism must properly notify downstream Service Providers, Contractors, and Third Parties if applicable.
3	Respond to a “Right to Delete” request	The dealer must put two or more mechanisms in place to respond to these types of requests it receives both online and in-person. This means responding to the consumer, employee or job applicant within the statutory deadlines. This mechanism must properly notify downstream Service Providers, Contractors, and Third Parties if applicable.
4	Respond to a “Right to Limit” request	The dealer must put two or more mechanisms in place to respond to these types of requests it receives both online and in-person. This means responding to the consumer, employee or job applicant within the statutory deadlines. This mechanism must properly notify downstream Service Providers, Contractors, and Third Parties if applicable.
5	Respond to a “Right to Opt-Out of Sale/Sharing” request	The dealer must put two or more mechanisms in place to respond to these types of requests it receives both online and in-person. This means responding to the consumer, employee or job applicant within the statutory deadlines and cannot require verification or authentication of the request. This mechanism must properly notify downstream Third Parties if applicable.
6	Respond to a “Right to Correct” request	The dealer must put two or more mechanisms in place to respond to these types of requests it receives both online and in-person. This means responding to the consumer, employee or job applicant within the statutory deadlines and cannot require verification or authentication of the request. This mechanism must properly notify downstream Service Providers, Contractors, and Third Parties if applicable.
7	Respond to a request by an Authorized Agent	The dealer must put a mechanism in place to verify the authorization as well as respond to the request as if it was made by the consumer, employee or job applicant themselves.

Disclosure Requirements		
#	Action	Notes
1	Privacy Policy	The privacy policy must have very specific disclosures as required by the CCPA.
2	Notice at Collection - Consumer (non-website)	The Notice at Collection provides the consumer with timely notice, at or before the time of collection, about the categories of personal information to be collected from them and the purposes for which the personal information is collected or used, and whether it is sold or shared. “Timely notice at or before the time of collection” can be interpreted to suggest that any telephone calls made or emails or promotions sent to consumers should have the Notice at Collection present.
3	Notice at Collection - Employee or Job Applicant (non-website)	The Notice at Collection provides the employee or job applicant with timely notice, at or before the time of collection, about the categories of personal information to be collected from them and the purposes for which the personal information is collected or used, and whether it is sold or shared. “Timely notice at or before the time of collection” can be interpreted to suggest that any emails sent to employees or job applicants should have the Notice at Collection present. Additionally, any job postings should have this notice as well.

Dealer Operations		
#	Action	Notes
1	Data Mapping and Systems Inventory	Dealers need to perform this in order to know how information flows through their organization and what is collected based on the consumer's, employee's or job applicant's interaction(s) with the dealer. Additionally, this map allows the dealer to identify the business purpose of collecting the information and which categories of third parties it shares this with.

2	Vendor Management - Service Provider	Each of the dealer's Service Providers must sign a contract that prohibits the use of customer information in certain ways. The contract has very specific requirements. Additionally, the dealer must maintain this Service Provider library in order to know which Service Provider to notify if it fulfills a consumer's, employee's, or job applicant's request.
3	Vendor Management - Third Parties	Each of the dealer's Third Parties must sign a contract that only allows it to use personal information for specific purposes. The dealer must maintain this Third Party library in order to know which Third Party to notify if it fulfills a consumer's, employee's, or job applicant's request.
4	Employee Training	Train all consumer-facing employees on the CCPA annually to ensure that they know what to do if they receive a request from a consumer.
5	Record-keeping	The dealer must maintain records of consumer requests for at least twenty-four (24) months.
6	Security Standards	In relation to this record-keeping requirement, the dealer must maintain reasonable security procedures and practices in maintaining the records. Additionally, dealers will be subject to civil liability by consumers if their non-encrypted and non-redacted personal information is subject to unauthorized access (i.e. a data breach).
7	Verification and Authentication	The dealer must establish a reasonable method for verifying the identity of a consumer if the consumer submits a request to delete, request to correct, or request to know. Note that this verification is not applicable to requests to opt-out of sale/sharing nor to limit the use of sensitive information.

Appendix C – SP/C Agreement

California Data Privacy Service Provider and Contractor Addendum

This California Data Privacy Addendum (“Addendum”) is between _____ (hereinafter referred to as “Service Provider” or “Contractor”) and _____ and/or any of its “Affiliated Entities” (hereinafter collectively referred to as “Dealer”) with which Service Provider or Contractor either (1) seeks to enter into a business relationship, or (2) has an existing business relationship. Affiliated Entities include any of Dealer’s existing or future franchises or businesses related by the same common branding, ownership or corporate control. This Addendum supplements and amends any and all existing agreements between Service Provider or Contractor and Dealer and constitutes a “Service Provider Contract” or “Contractor Contract” subject to the CCPA. To the extent of any ambiguity or conflict between any other agreement and this Addendum, the terms of this Addendum shall apply; otherwise, the terms of any underlying agreement shall remain in full force and effect. This Addendum shall be effective as of the date the document is executed below by Dealer. If any provision of this Addendum is found invalid or unenforceable, all remaining provisions of this Addendum will remain in full force and effect. It shall remain in effect until either revoked in writing or automatically if the business relationship between Dealer and Service Provider or Contractor comes to an end, except that the representations and warranties listed in Sections 3 and 4 of this agreement shall survive any termination.

1. **Personal Information.** For purposes of this Addendum, “Personal Information” shall mean any information that Service Provider or Contractor receives, access, collects, or processes pursuant to an existing agreement between Dealer and Service Provider or Contractor, where the information identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, to a particular consumer or household, including, but not limited to, all categories of personal information defined under the California Consumer Privacy Act (CCPA), Cal. Civ. Code §1798.100 et seq. and accompanying regulations.
2. **Identification of Specified Business Purposes.** Pursuant to the existing agreement(s) between Dealer and Service Provider or Contractor, Service Provider or Contractor represents that it processes Personal Information for the following “Business Purposes” defined under the CCPA and its accompanying regulations (*check all that apply*):
 - Auditing related to counting ad impressions to unique visitors, verifying positioning and quality of ad impressions, and auditing compliance with this specification and other standards.
 - Helping to ensure security and integrity to the extent the use of the consumer’s personal information is reasonably necessary and proportionate for these purposes.
 - Debugging to identify and repair errors that impair existing intended functionality.
 - Short-term, transient use, including, but not limited to, non-personalized advertising shown as part of a consumer’s current interaction with Dealer, provided that the consumer’s personal information is not disclosed to another third party and is not used to build a profile about the consumer or otherwise alter the consumer’s experience outside the current interaction with Dealer.
 - Performing services on behalf of the Dealer, including maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing financing, providing analytic services, providing storage, or providing similar services on behalf of the Dealer.
 - Providing advertising and marketing services, excluding cross-contextual behavioral advertising.
 - Undertaking internal research for technological development and demonstration.
 - Undertaking activities to verify or maintain the quality or safety of a service or device that is owned, manufactured, manufactured for, or controlled by Dealer, and to improve, upgrade, or enhance the service or device that is owned, manufactured, manufactured for, or controlled by Dealer.
3. **Service Provider or Contractor Restrictions** In accordance with the CCPA, Service Provider or Contractor is hereby prohibited from:
 - a. Selling or sharing Personal Information.

- b. Retaining, using, or disclosing the Personal Information for any purpose other than for performing the Business Purpose(s) specified in Section 2 above for Dealer, or as otherwise expressly permitted by CCPA and its accompanying regulations.
 - c. Retaining, using, or disclosing Personal Information outside of the direct business relationship between Service Provider or Contractor and Dealer.
 - d. Combining Personal Information that Service Provider or Contractor receives from, or on behalf of, the business with Personal Information that it receives from, or on behalf of, another person or persons, or collects from its own interactions with consumers, except as otherwise expressly permitted by the CCPA and its accompanying regulations.
 - e. Using Personal Information to engage in retargeting advertising or cross-contextual behavioral advertising.
- 4. Service Provider or Contractor Obligations.** Service Provider or Contractor shall:
- a. Comply with all applicable sections of the CCPA and its accompanying regulations, including—with respect to Personal Information that it collects—providing the same level of privacy protection as required by Dealer by the CCPA and its accompanying regulations.
 - b. Cooperate with Dealer in responding to and complying with consumers' requests made pursuant to the CCPA, and to implementing reasonable security procedures and practices appropriate to the nature of the personal information received from, or on behalf of, the business to protect the personal information from unauthorized or illegal access, destruction, use, modification, or disclosure in accordance with Civil Code § 1798.81.5.
 - c. Notify Dealer as soon as practicable after Service Provider or Contractor makes a determination that it can no longer meet its obligations under the CCPA and these regulations.
 - d. Upon written notice by Dealer, take reasonable and appropriate steps to stop and remediate Service Provider's or Contractor's use of Personal Information that violates the terms of this Addendum.
- 5. Risk Assessments.** Service Provider or Contractor will, upon Dealer's request, but no more than once per year, satisfactorily complete a reasonable questionnaire that demonstrates Service Provider's or Contractor's ability to comply with Section 2 through 4 above, provided that such questionnaire is not unduly burdensome to Service Provider or Contractor.
- 6. Execution & Enforceability.** By signing below, Service Provider or Contractor acknowledges and agrees that (1) a digital copy of this signed Addendum will be made available to the Dealer and (2) the Addendum shall become legally binding upon a Dealer countersigning the Addendum. This Addendum shall only be valid and legally binding if Service Provider or Contractor and Dealer are parties to an underlying commercial agreement at the time of execution by Dealer where Service Provider or Contractor receives, maintains, processes, or otherwise is permitted access to Customer Information through its provision of services. Service Provider or Contractor and Dealer agree that this Addendum may be signed and/or transmitted by electronic mail of a PDF document or electronic signature (e.g., DocuSign or similar electronic signature technology) and thereafter maintained in electronic form, and that such electronic record shall be valid and effective to bind the party so signing as a paper copy bearing such party's hand-written signature.

Service Provider or Contractor

Signature: _____

Printed Name: _____

Title: _____

Date: _____

Dealer**Signature:**

Printed Name:

Title:

Date:

SAMPLE
NOT FOR REPRODUCTION

Appendix D – Third Party Agreement

California Data Privacy Service Third Party Addendum

This California Data Privacy Addendum (“Addendum”) is between _____ (hereinafter referred to as “Third Party”) and _____ and/or any of its “Affiliated Entities” (hereinafter collectively referred to as “Dealer”) with which Service Provider either (1) seeks to enter into a business relationship, or (2) has an existing business relationship. Affiliated Entities include any of Dealer’s existing or future franchises or businesses related by the same common branding, ownership or corporate control. This Addendum supplements and amends any and all existing agreements between Third Party and Dealer and constitutes a “Third Party contract” subject to the CCPA and its accompanying regulations. To the extent of any ambiguity or conflict between any other agreement and this Addendum, the terms of this Addendum shall apply; otherwise, the terms of any underlying agreement shall remain in full force and effect. This Addendum shall be effective as of the date the document is executed below by Dealer. If any provision of this Addendum is found invalid or unenforceable, all remaining provisions of this Addendum will remain in full force and effect. It shall remain in effect until either revoked in writing or automatically if the business relationship between Dealer and Service Provider comes to an end, except that the representations and warranties listed in Sections 3 and 4 of this agreement shall survive any termination.

1. **Personal Information.** For purposes of this Addendum, “Personal Information” shall mean any information that Third Party receives, access, collects, or processes pursuant to an existing agreement between Dealer and Third Party, where the information identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, to a particular consumer or household, including, but not limited to, all categories of personal information defined under the CCPA and its accompanying regulations.
2. **Identification of Specified Purpose(s).** Pursuant to the existing agreement(s) between Dealer and Third Party, Third Party represents that it sells and/or shares Personal Information for the following Specific Purpose(s) (*check all that apply*):
 - Online retargeting advertising, cross-context behavioral advertising, or similar digital marketing services.
 - Geofencing, geotargeting or other location-based marketing services.
 - Data analytics, reporting or similar services.
 - Equity mining, data mining or similar services.
 - Sales prospecting and lead generation.
 - Advertising or marketing of products and services through email, mailers, text messages or similar services.
 - Reputation and brand management, customer experience and satisfaction improvement or similar services.
 - Other: _____
3. **Third Party Restrictions** In accordance with the CCPA and its accompanying regulations, Third Party is hereby prohibited from:
 - a. Retaining, using, or disclosing the Personal Information for any purpose other than for the limited and Specific Purpose(s) specified in Section 2 above for Dealer, or as otherwise expressly permitted by the CCPA and its accompanying regulations.
4. **Third Party Obligations.** Third Party shall:
 - a. Comply with all applicable sections of the CCPA and its accompanying regulations, including—with respect to Personal Information that it collects—providing the same level of privacy protection as required by Dealer by the CCPA and its accompanying regulations.
 - b. Cooperate with Dealer in responding to and complying with consumers’ requests made pursuant to the CCPA, and to implementing reasonable security procedures and practices appropriate to the nature of the personal information received from, or on behalf of, the business to protect the personal information from unauthorized or illegal access, destruction, use, modification, or disclosure in accordance with Civil Code § 1798.81.5.

- c. Notify Dealer as soon as practicable after the Third Party makes a determination that it can no longer meet its obligations under the CCPA and its accompanying regulations.
 - d. Upon written notice by Dealer, take reasonable and appropriate steps to stop and remediate Third Party's use of Personal Information that violates the terms of this Addendum.
5. **Risk Assessments.** Third Party will, upon Dealer's request, but no more than once per year, satisfactorily complete a reasonable questionnaire that demonstrates Third Party's ability to comply with Section 2 through 4 above, provided that such questionnaire is not unduly burdensome to Third Party.
6. **Execution & Enforceability.** By signing below, Third Party acknowledges and agrees that (1) a digital copy of this signed Addendum will be made available to the Dealer and (2) the Addendum shall become legally binding upon a dealer countersigning the Addendum. This Addendum shall only be valid and legally binding if Third Party and Dealer are parties to an underlying commercial agreement at the time of execution by Dealer where Third Party receives, maintains, processes, or otherwise is permitted access to Customer Information through its provision of services. Third Party and Dealer agree that this Addendum may be signed and/or transmitted by electronic mail of a PDF document or electronic signature (e.g., DocuSign or similar electronic signature technology) and thereafter maintained in electronic form, and that such electronic record shall be valid and effective to bind the party so signing as a paper copy bearing such party's hand-written signature.

Third Party

Signature: _____

Printed Name: _____

Title: _____

Date: _____

Dealer

Signature: _____

Printed Name: _____

Title: _____

Date: _____

NOT FOR REPRODUCTION
SAMPLE