



CCPA Self- Assessment Compliance Report

A Review of Thoropass's Compliance Against
the California Consumer Privacy Act (CCPA)
(Final Regulations - March 29, 2023)

April 14, 2023; Updated/Reviewed April 15, 2024

Mailing Address:

228 Park Ave S., PMB 41082,
New York, NY 10003

Table of Contents

Table of Contents	1
1 Introduction	3
1.1 Background	3
1.2 Overview	3
1.3 Objectives	3
1.4 Regulated Business	3
2 Executive Summary	4
2.1 Scope	4
2.2 Methodology	4
2.3 Findings and Recommendations	5
2.4 Overall Summary	5
3 Report Details	9
Article 1 General Provisions	9
7000 Title and Scope	9
7001 Definitions	9
7002 Restrictions on the Collection and Use of Personal Information	9
7003 Requirements for Disclosures and Communications to Consumers	12
7004 Requirements for Methods for Submitting CCPA Requests and Obtaining Consumer Consent	14
Article 2 Required Disclosures to Consumers	15
7010 Overview of Required Disclosures	15
7011 Privacy Policy	16
7012 Notice at Collection of Personal Information	20
7013 Notice of Right to Opt-out of Sale/Sharing and the “Do Not Sell or Share My Personal Information” Link	23
7014 Notice of Right to Limit and the “Limit the Use of My Sensitive Personal Information” Link	26
7015 Alternative Opt-out Link	29
7016 Notice of Financial Incentive	30
Article 3 Business Practices for Handling Consumer Requests	31
7020 Methods for Submitting Requests to Delete, Requests to Correct, and Requests to Know	31
7021 Timelines for Responding to Requests to Delete, Requests to Correct, and Requests to Know	33
7022 Requests to Delete	34
7023 Requests to Correct	38
7024 Requests to Know	43
7025 Opt-out Preference Signals	48
7026 Requests to Opt-out of Sale/Sharing	51
7027 Requests to Limit Use and Disclosure of Sensitive Personal Information	55

7028 Requests to Opt-in After Opting-out of the Sale or Sharing of Personal Information	59
Article 4 Service Providers, Contractors, and Third Parties	60
7050 Service Providers and Contractors	60
7051 Contract Requirements for Service Providers and Contractors	63
7052 Third Parties	65
7053 Contract Requirements for Third Parties	66
Article 5 Verification of Requests	67
7060 General Rules Regarding Verification	67
7061 Verification for Password-Protected Accounts	71
7062 Verification for Non-Accountholders	71
7063 Authorized Agents	74
Article 6 Special Rules Regarding Consumers Under 16 Years of Age	75
7070 Consumers Less Than 13 Years of Age	75
7071 Consumers at Least 13 Years of Age and Less Than 16 Years of Age	76
7072 Notices to Consumers Less Than 16 Years of Age	77
Article 7 Non-Discrimination	78
7080 Discriminatory Practices	78
7081 Calculating the Value of Consumer Data	80
Article 8 Training and Record-Keeping	81
7100 Training	81
7101 Record-Keeping	82
7102 Requirements for Businesses Collecting Large Amounts of Personal Information	83
Article 9 Investigation and Enforcement	84
7300 Sworn Complaints Filed with the Agency	84
7301 Investigations	85
7302 Probable Cause Proceedings	85
7303 Stipulated Orders	86
7304 Agency Audits	86
Appendices	88
Appendix A - Project Team	88
Appendix B - List of Evidence Reviewed	88

1 Introduction

1.1 Background

The California Consumer Privacy Act of 2018 (CCPA) provides more privacy rights for California consumers giving them more control over the personal information businesses collect. These rights include:

- The right to know about the personal information collected about them by a business and how their personal information is used or shared;
- The right to delete their personal information;
- The right to opt-out of sale of their personal information; and
- The right to not be discriminated against for exercising their rights.

1.2 Overview

This CCPA Compliance Report consists of a self-assessment performed by an experienced and qualified assessor during the review period of April 5, 2023 to April 14, 2023 (updated and annual review performed April 15, 2024).

Without defined policies and privacy over information systems, Thoropass's ability to conduct business may be impacted. The preservation of Thoropass's reputation is directly linked to the management over the privacy of Thoropass's information. Thoropass's primary concern related to privacy is the use and disclosure of personal data.

1.3 Objectives

The objective of this review was to verify Thoropass's policies, standards, and procedures meeting the objectives outlined in the CCPA and the California Code of Regulations (CCR) issued by the California Privacy Protection Agency with their final rule release of March 29, 2023. In addition, the objective of this review was to verify Thoropass's management and employees ensure appropriate compliance with the articles outlined in the CCPA.

1.4 Regulated Business

Although Thoropass does not currently meet the following criteria to be considered a Business under the provisions of the CCPA: have a gross annual revenue of over \$25 million; buys, receives, or sells the personal information of 50,000 or more California residents, households, or devices; or derives 50% or more of its annual revenue from selling California residents' personal information; Thoropass is a for-profit business conducting business in California supporting other Businesses as a service provider (and/or contractor). Thoropass has **VOLUNTARILY** obligated itself to comply with the CCPA Regulations. Thoropass plans to certify with the CPPA its compliance with and agrees to be bound by the CCPA.

2 Executive Summary

Overall, Thoropass's compliance posture with the CCPA meets compliance requirements to protect Thoropass's information systems and personal data. Thoropass has noted a couple of items to consider. These findings and recommendations are discussed in detail in Section 3 of this report and summarized in Section 2.3 below.

2.1 Scope

This assessment reviewed the use, disclosure, and accessibility of personal data available to authorized individuals. This assessment reviewed the articles of the CCPA summarized under Section 2.4 below.

The scope of this review included:

- The Thoropass's policies and procedures related to CCPA Compliance.
- The Thoropass's information system and platform maintaining personal data to include cloud hosting environment(s): Amazon Web Services (AWS)
- This assessment include the following location: 159 W 25th Street, (7th Floor), New York, NY 10001

2.2 Methodology

Thoropass conducted a process-based review focusing on the significant objectives of CCPA compliance. Thoropass reviewed the nine (9) articles and thirty-seven (37) regulations documented in the CCPA. Thoropass utilized these regulations to collect evidence in sufficient quantity/quality to validate conformity. The use of these procedures provide a systematic way to perform assessments reducing the risk of errors and reinforcing the objectivity of the assessment's conclusions. Recommendations were provided according to regulatory requirements, standards, frameworks, industry best practices, and experience from subject matter experts.

This assessment covers the following accountability principles outlined in the CCPA articles to include, but not limited to:

1. Notices to Consumers
2. Business Practices for Handling Consumer Requests
3. Verification of Requests
4. Special Rules Regarding Consumers Under 16 Years of Age
5. Non-Discrimination

2.3 Findings and Recommendations

The following items were identified during this review in need of improvements:

1. **Regulation 7003b** - **Partially Compliant** - Thoropass performs web accessibility automated testing prior to publishing the website to the Internet. Thoropass should provide additional demonstrable evidence to validate the <https://thoropass.com> website conforms to the Web Content Accessibility Guidelines, version 2.1 of June 5, 2018, from the World Wide Web Consortium for reasonable accessibility to consumers with disabilities. *Note: Thoropass will be undergoing a full accessibility review and mitigation process in the future.*

2.4 Overall Summary

The CCPA regulations were assigned a compliance status defined as follows:

- **Applicable** - The regulation applies to Thoropass, but there isn't evidence required to prove compliance.
- **Fully Compliant** - Thoropass meets all criteria of the requirement.
- **Partially Compliant** - Thoropass meets some criteria of the requirement, but needs to improve compliance efforts based on the recommendations provided.
- **Not Compliant** - Thoropass does not meet the criteria of the requirements; recommendations are provided for consideration.
- **Not Applicable (N/A)** - the regulation doesn't apply to Thoropass.

The following table provides a summary of Thoropass's compliance status against the CCPA requirements:

Article 1 General Provisions						
7000 Title and Scope						
7001 Definitions						
7002 Restrictions on the Collection and Use of Personal Information						
a	b	c	d	e	f	
7003 Requirements for Disclosures and Communications to Consumers						
a	b	c	d			
7004 Requirements for Methods for Submitting CCPA Requests and Obtaining Consumer Consent						
a	b	c				
Article 2 Required Disclosures to Consumers						
7010 Overview of Required Disclosures						
a	b	c	d	e		
7011 Privacy Policy						
a	b	c	d	e		
7012 Notice at Collection of Personal Information						
a	b	c	d	e	f	g
h	i					
7013 Notice of Right to Opt-out of Sale/Sharing and the “Do Not Sell or Share My Personal Information” Link						
a	b	c	d	e	f	g
h						
7014 Notice of Right to Limit and the “Limit the Use of My Sensitive Personal Information” Link						
a	b	c	d	e	f	g
h						
7015 Alternative Opt-out Link						
a	b	c				
7016 Notice of Financial Incentive						
a	b	c	d			
Article 3 Business Practices for Handling Consumer Requests						
7020 Methods for Submitting Requests to Delete, Requests to Correct, and Requests to Know						
a	b	c	d	e		
7021 Timelines for Responding to Requests to Delete, Requests to Correct, and Requests to Know						
a	b					
7022 Requests to Delete						
a	b	c	d	e	f	g

h						
7023 Requests to Correct						
a	b	c	d	e	f	g
h	i	j	k			
7024 Requests to Know						
a	b	c	d	e	f	g
h	i	j	k	l		
7025 Opt-out Preference Signals						
a	b	c	d	e	f	g
7026 Requests to Opt-out of Sale/Sharing						
a	b	c	d	e	f	g
h	i	j	k			
7027 Requests to Limit Use and Disclosure of Sensitive Personal Information						
a	b	c	d	e	f	g
h	i	j	k	l	m	
7028 Requests to Opt-in After Opting-out of the Sale or Sharing of Personal Information.						
a	b					
Article 4 Service Providers, Contractors, and Third Parties						
7050 Service Providers and Contractors						
a	b	c	d	e	f	g
7051 Contract Requirements for Service Providers and Contractors						
a	b	c				
7052 Third Parties						
a	b					
7053 Contract Requirements for Third Parties						
a	b					
Article 5 Verification of Requests						
7060 General Rules Regarding Verification						
a	b	c	d	e	f	g
h						
7061 Verification for Password-Protected Accounts						
a	b					
7062 Verification for Non-Accountholders						
a	b	c	d	e	f	g
7063 Authorized Agents.						
a	b	c	d			

Article 6 Special Rules Regarding Consumers Under 16 Years of Age						
7070 Consumers Less Than 13 Years of Age						
a	b	c				
7071 Consumers at Least 13 Years of Age and Less Than 16 Years of Age						
a	b					
7072 Notices to Consumers Less Than 16 Years of Age						
a	b					
Article 7 Non-Discrimination						
7080 Discriminatory Practices						
a	b	c	d	e	f	g
7081 Calculating the Value of Consumer Data						
a	b					
Article 8 Training and Record-Keeping						
7100 Training						
a	b					
7101 Record-Keeping						
a	b	c	d	e		
7102 Requirements for Businesses Collecting Large Amounts of Personal Information						
a	b					
Article 9 Investigation and Enforcement						
7300 Sworn Complaints Filed with the Agency						N/A
7301 Investigations						N/A
7302 Probable Cause Proceedings						N/A
7303 Stipulated Orders						N/A
7304 Agency Audits						N/A

3 Report Details

Article 1 General Provisions

7000 Title and Scope

Applicable	Evidence: N/A
<p>Regulation: (a) This Chapter shall be known as the California Consumer Privacy Act Regulations. It may be cited as such and will be referred to in this Chapter as “these regulations.” These regulations govern compliance with the California Consumer Privacy Act and do not limit any other rights that consumers may have. (b) A violation of these regulations shall constitute a violation of the CCPA and be subject to the remedies provided for therein.</p>	
<p>Observations/Findings: Thoropass: does not currently have annual gross revenue in excess of twenty-five (25) million dollars; does not annually buy, sell, or share personal information of 100,000 or more consumers; and does not derive fifty percent (50%) or more of its annual revenue from selling or sharing consumers' personal information; however, Thoropass does business in California and has VOLUNTARILY obligated itself to the California Consumer Privacy Act (CCPA) Regulations. Thoropass plans to certify to the California Privacy Protection Agency (CPPA) its compliance with and agrees to be bound by the CCPA.</p>	
<p>Recommendations: No further recommendations at this time.</p>	

7001 Definitions

Applicable	Evidence: N/A
<p>Regulation: [Encompasses definitions set forth under this regulation, Civil Code section 1798.140 and 1798.145.]</p>	
<p>Observations/Findings: Thoropass is bound by the definitions set forth in Civil Code section 1798.140 and 1798.145</p>	
<p>Recommendations: No further recommendations at this time.</p>	

7002 Restrictions on the Collection and Use of Personal Information

A Fully Compliant	Evidence: Online Privacy Notice; Data Protection Impact Assessment (DPIA)
<p>Regulation: (a) In accordance with Civil Code section 1798.100, subdivision (c), a business's collection, use, retention, and/or sharing of a consumer's personal information shall be reasonably necessary and proportionate to achieve: (1) The purpose(s) for which the personal information was collected or processed, which shall comply with the requirements set forth in subsection (b); or (2) Another disclosed purpose that is compatible with the context in which the personal information was</p>	

collected, which shall comply with the requirements set forth in subsection (c).

Observations/Findings: Thoropass reasonably and proportionately collects, uses, retains, and/or shares consumers' personal information to achieve its purpose for which the personal information was collected or processed. Thoropass provides a Privacy Notice to consumers through its website at the time of collection detailing the purpose of collection, use, retention, and/or sharing of consumers' personal information. Thoropass performs a data protection impact assessment, which includes an assessment on proportionality.

Recommendations: No further recommendations at this time.

B Fully Compliant

Evidence: Online Privacy Notice; Data Protection Impact Assessment (DPIA); Sub-processor List

Regulation:

(b) The purpose(s) for which the personal information was collected or processed shall be consistent with the reasonable expectations of the consumer(s) whose personal information is collected or processed. The consumer's (or consumers') reasonable expectations concerning the purpose for which their personal information will be collected or processed shall be based on the following:

- (1) The relationship between the consumer(s) and the business.
- (2) The type, nature, and amount of personal information that the business seeks to collect or process.
- (3) The source of the personal information and the business's method for collecting or processing it.
- (4) The specificity, explicitness, prominence, and clarity of disclosures to the consumer(s) about the purpose for collecting or processing their personal information, such as in the Notice at Collection and in the marketing materials to the consumer(s) about the business's good or service.
- (5) The degree to which the involvement of service providers, contractors, third parties, or other entities in the collecting or processing of personal information is apparent to the consumer(s).

Observations/Findings: Thoropass collects or processes personal information consistent with the reasonable expectation of consumers whose personal information is collected or processed. This reasonable expectation is based on:

1. Thoropass's relationship with the consumer;
2. The type, nature, and amount of personal information Thoropass seeks to collect or process;
3. The source of personal information and the method Thoropass uses to collect or process the information;
4. The specificity, explicitness, prominence, and clarity of disclosures about the purpose for collecting/processing personal information; and (*Note: Thoropass provides a Privacy Notice at the time of collection and on all marketing material provided to consumers about Thoropass's goods and services.*)
5. The degree to which service providers, contractors, third parties, or other entities are involved in collecting/processing personal information on Thoropass's behalf as provided for in the Privacy Policy detailing sub-processor involvement.

Recommendations: No further recommendations at this time.

C Not Applicable

Evidence: N/A

Regulation:

(c) Whether another disclosed purpose is compatible with the context in which the personal information was collected shall be based on the following:

- (1) At the time of collection of the personal information, the reasonable expectations of the consumer(s) whose personal information is collected or processed concerning the purpose for which their personal

information will be collected or processed, based on the factors set forth in subsection (b).
 (2) The other disclosed purpose for which the business seeks to further collect or process the consumer's personal information, including whether it is a business purpose listed in Civil Code section 1798.140, subdivisions (e)(1) through (e)(8).
 (3) The strength of the link between subsection (c)(1) and subsection (c)(2).

Observations/Findings: N/A. Thoropass fully discloses the purpose of collection under reasonable expectations and does not collect or process personal information other than what is permitted for specific purposes as disclosed in Thoropass's Privacy Policy.

Recommendations: Not applicable.

D Fully Compliant

Evidence: Online Privacy Notice; PT-01 Privacy Policy

Regulation:

(d) For each purpose identified in compliance with subsection (a)(1) or (a)(2), the collection, use, retention, and/or sharing of a consumer's personal information to achieve that purpose shall be reasonably necessary and proportionate. The business's collection, use, retention, and/or sharing of a consumer's personal information shall also be reasonably necessary and proportionate to achieve any purpose for which the business obtains the consumer's consent in compliance with subsection (e). Whether a business's collection, use, retention, and/or sharing of a consumer's personal information is reasonably necessary and proportionate to achieve the purpose identified in compliance with subsection (a)(1) or (a)(2), or any purpose for which the business obtains consent, shall be based on the following:
 (1) The minimum personal information that is necessary to achieve the purpose identified in compliance with subsection (a)(1) or (a)(2), or any purpose for which the business obtains consent.
 (2) The possible negative impacts on consumers posed by the business's collection or processing of the personal information.
 (3) The existence of additional safeguards for the personal information to specifically address the possible negative impacts on consumers considered by the business in subsection (d)(2).

Observations/Findings: Thoropass only collects, uses, retains, and/or shares consumers' personal information to achieve its intended processing purpose in a reasonably necessary and proportionate manner. Thoropass collects, uses, retains, and/or shares consumers' personal information under consent by the consumer based on the following:
 1. Thoropass only uses the minimum necessary personal information to achieve the disclosed purpose for which Thoropass obtains consent;
 2. Thoropass notifies consumers of any negative impact on the consumer posed by collection or processing of their personal information; and
 3. Thoropass implements safeguards over personal information such as encryption and restricted access to address any negative impacts on consumers identified by Thoropass.

Recommendations: No further recommendations at this time.

E Fully Compliant

Evidence: PT-04 Consent; Consent Evidence

Regulation:

(e) A business shall obtain the consumer's consent in accordance with section 7004 before collecting or processing personal information for any purpose that does not meet the requirements set forth in subsection (a).

Observations/Findings: Thoropass obtains consumers' consent before collecting or processing

personal information for any purpose.

Recommendations: No further recommendations at this time.

F Fully Compliant **Evidence:** Online Privacy Notice

Regulation:

(f) A business shall not collect categories of personal information other than those disclosed in its Notice at Collection in accordance with the CCPA and section 7012. If the business intends to collect additional categories of personal information or intends to use the personal information for additional purposes that are incompatible with the disclosed purpose for which the personal information was collected, the business shall provide a new Notice at Collection. However, any additional collecting or processing of personal information shall comply with subsection (a).

Observations/Findings: Thoropass only collects categories of personal information disclosed in the Privacy Policy (i.e. Notice at Collection) at the time of collection according to the CCPA. Thoropass restricts the collection of personal information that is not disclosed in the notice. If Thoropass intends to collect additional categories, Thoropass provides a new notice at collection. Thoropass's privacy notice contains the following:

- A list of the categories of personal information about consumers to be collected. Each category of personal information is written in a manner providing consumers a meaningful understanding of the information being collected.
- The business or commercial purpose(s) for which the categories of personal information will be used.
- Thoropass does not sell personal information.
- A link to Thoropass's privacy policy/notice, or in the case of offline notices, where the privacy policy/notice can be found online.

The notice at collection is readily available where consumers encounter it at or before the point of collection of any personal information. If Thoropass unexpectedly collects personal information from a consumer's mobile device, Thoropass provides a just-in-time notice containing a summary of categories and a link to the full notice.

Recommendations: No further recommendations at this time.

7003 Requirements for Disclosures and Communications to Consumers

A Fully Compliant **Evidence:** Online Privacy Notice

Regulation:

(a) Disclosures and communications to consumers shall be easy to read and understandable to consumers.

Observations/Findings: Thoropass's Privacy Notice is written in plain, straightforward language, and avoids technical/legal jargon.

Recommendations: No further recommendations at this time.

B Partially Compliant **Evidence:** Online Privacy Notice

Regulation:

(b) Disclosures required under Article 2 shall also:
 (1) Use a format that makes the disclosure readable, including on smaller screens, if applicable.
 (2) Be available in the languages in which the business in its ordinary course provides contracts, disclaimers, sale announcements, and other information to consumers in California.
 (3) Be reasonably accessible to consumers with disabilities. For notices provided online, the business shall follow generally recognized industry standards, such as the Web Content Accessibility Guidelines, version 2.1 of June 5, 2018, from the World Wide Web Consortium, incorporated herein by reference. In other contexts, the business shall provide information on how a consumer with a disability may access the policy in an alternative format.

Observations/Findings: Thoropass's Privacy Notice is in a format drawing the consumer's attention to the notice and makes the notice readable (including on smaller screens, if applicable). The privacy notice is available in the language (English) in which Thoropass in its ordinary course provides contracts, disclaimers, sale announcements, and other information to consumers in California.

The privacy notice is reasonably accessible to consumers with disabilities. Thoropass abides by Web Content Accessibility Guidelines (WCAG), version 2.1 of June 5, 2018, from the World Wide Web Consortium. Thoropass provides information on how a consumer with a disability may access the notice in an alternative format.

Recommendations: Thoropass performs web accessibility automated testing prior to publishing the website to the Internet. Thoropass should provide additional demonstrable evidence to validate the <https://thoropass.com> website conforms to the Web Content Accessibility Guidelines, version 2.1 of June 5, 2018, from the World Wide Web Consortium for reasonable accessibility to consumers with disabilities. *Note: Thoropass will be undergoing a full accessibility review and mitigation process in the future.*

C Fully Compliant	Evidence: Online Privacy Notice
Regulation: (c) For websites, a conspicuous link required under the CCPA or these regulations shall appear in a similar manner as other similarly-posted links used by the business on its homepage(s).	
Observations/Findings: Thoropass provides a conspicuous link on its website to the Privacy Notice located at https://thoropass.com/privacy-policy/ as required under the CCPA.	
Recommendations: No further recommendations at this time.	

D Not Applicable	Evidence: N/A
Regulation: (d) For mobile applications, a conspicuous link shall be included in the business's privacy policy, which must be accessible through the mobile application's platform page or download page. It may also be accessible through a link within the application, such as through the application's settings menu.	
Observations/Findings: N/A. Thoropass does not develop a mobile application for use by consumers.	
Recommendations: Not applicable.	

7004 Requirements for Methods for Submitting CCPA Requests and Obtaining Consumer Consent

A Fully Compliant

Evidence: Online Privacy Notice

Regulation:

(a) Except as expressly allowed by the CCPA and these regulations, businesses shall design and implement methods for submitting CCPA requests and obtaining consumer consent that incorporate the following principles:

- (1) Easy to understand. The methods shall use language that is easy for consumers to read and understand. When applicable, they shall comply with the requirements for disclosures to consumers set forth in section 7003.
- (2) Symmetry in choice. The path for a consumer to exercise a more privacy-protective option shall not be longer or more difficult or time-consuming than the path to exercise a less privacy-protective option because that would impair or interfere with the consumer's ability to make a choice.
- (3) Avoid language or interactive elements that are confusing to the consumer. The methods should not use double negatives. Toggles or buttons must clearly indicate the consumer's choice.
- (4) Avoid choice architecture that impairs or interferes with the consumer's ability to make a choice. Businesses should also not design their methods in a manner that would impair the consumer's ability to exercise their choice because consent must be freely given, specific, informed, and unambiguous.
- (5) Easy to execute. The business shall not add unnecessary burden or friction to the process by which the consumer submits a CCPA request. Methods should be tested to ensure that they are functional and do not undermine the consumer's choice to submit the request.

Observations/Findings: Thoropass designs and implements methods to submit CCPA requests and obtain consent incorporating the following principles:

1. Thoropass makes disclosures easy to understand using language easy for consumers to read;
2. Thoropass does not make the path for a consumer to exercise more privacy-protection options longer, more difficult, or time-consuming than the path to exercise less privacy-protection options. Thoropass does not impair or interfere with a consumer's ability to make a choice;
3. Thoropass avoids language or interactive elements causing confusion with consumers such as the use of double negatives. Toggles or buttons provided clearly indicate a consumer's choice;
4. Thoropass avoided choice architecture impairing or interfering with the consumer's ability to make a choice. Thoropass provides for the ability of consumers to exercise their choice through freely given, specific, informed, and unambiguous consent; and
5. Thoropass does not add unnecessary burden or friction to the process for consumers to submit a CCPA request making any request easy to execute. Thoropass tests methods to ensure they function and do not undermine a consumer to submit a request.

Note: Thoropass has not received any CCPA related requests from any consumers over the last twelve (12) months.

Recommendations: No further recommendations at this time.

B Fully Compliant

Evidence: Online Privacy Notice

Regulation:

(b) A method that does not comply with subsection (a) may be considered a dark pattern. Any agreement obtained through the use of dark patterns shall not constitute consumer consent.

Observations/Findings: Thoropass does not sell personal information and states this in their privacy notice (under Right to Opt Out of the California Privacy Rights section). Thoropass does not utilize dark pattern methods to obtain consent.

Recommendations: No further recommendations at this time.

C Fully Compliant **Evidence:** Online Privacy Notice

Regulation:

(c) A user interface is a dark pattern if the interface has the effect of substantially subverting or impairing user autonomy, decision making, or choice. A business's intent in designing the interface is not determinative in whether the user interface is a dark pattern, but a factor to be considered. If a business did not intend to design the user interface to subvert or impair user choice, but the business knows of and does not remedy a user interface that has that effect, the user interface may still be a dark pattern. Similarly, a business's deliberate ignorance of the effect of its user interface may also weigh in favor of establishing a dark pattern.

Observations/Findings: Thoropass does not sell personal information and states this in their privacy notice (under Right to Opt Out of the California Privacy Rights section). Thoropass does not utilize dark pattern methods to obtain consent.

Recommendations: No further recommendations at this time.

Article 2 Required Disclosures to Consumers

7010 Overview of Required Disclosures

A Fully Compliant **Evidence:** Online Privacy Notice

Regulation:

(a) Every business that must comply with the CCPA and these regulations shall provide a privacy policy in accordance with the CCPA and section 7011.

Observations/Findings: Thoropass provides a Privacy Notice located at <https://thoropass.com/privacy-policy/> as required under the CCPA.

Recommendations: No further recommendations at this time.

B Fully Compliant **Evidence:** Online Privacy Notice

Regulation:

(b) A business that controls the collection of a consumer's personal information from a consumer shall provide a Notice at Collection in accordance with the CCPA and section 7012.

Observations/Findings: Thoropass provides a Privacy Notice (i.e. Notice at Collection) at the time of collection of a consumer's personal information.

Recommendations: No further recommendations at this time.

C Not Applicable **Evidence:** N/A

Regulation: (c) Except as set forth in section 7025, subsection (g), a business that sells or shares personal information shall provide a Notice of Right to Opt-out of Sale/Sharing or the Alternative Opt-out Link in accordance with the CCPA and sections 7013 and 7015.	
Observations/Findings: N/A. Thoropass does not sell personal information (or share personal information for cross-context behavioral advertising) to third-parties.	
Recommendations: Not applicable.	

D Not Applicable	Evidence: N/A
Regulation: (d) A business that uses or discloses a consumer's sensitive personal information for purposes other than those specified in section 7027, subsection (m), shall provide a Notice of Right to Limit or the Alternative Opt-out Link in accordance with the CCPA and sections 7014 and 7015.	
Observations/Findings: N/A. Thoropass does not use or disclose a consumer's sensitive personal information for any other purposes besides those to provide services or goods reasonably expected by an average consumer who requests those goods or services from Thoropass. Thoropass is not required to post a Notice of Right to Limit, an Alternative Opt-out Link, or provide a method for submitting a request to limit.	
Recommendations: Not applicable.	

E Not Applicable	Evidence: N/A
Regulation: (e) A business that offers a financial incentive or price or service difference shall provide a Notice of Financial Incentive in accordance with the CCPA and section 7016.	
Observations/Findings: N/A. Thoropass does not offer a financial incentive (or price/service difference) on its goods/services. Thoropass is not required to provide a Notice of Financial Incentive.	
Recommendations: Not applicable.	

7011 Privacy Policy

A Fully Compliant	Evidence: Online Privacy Notice
Regulation: (a) The purpose of the privacy policy is to provide consumers with a comprehensive description of a business's online and offline information practices. It shall also inform consumers about the rights they have regarding their personal information and provide any information necessary for them to exercise those rights.	
Observations/Findings: Thoropass's Privacy Notice provides consumers with a comprehensive description of Thoropass's online (and offline) information practices. The Privacy Notice informs consumers of their rights regarding their personal information and provides information on how they can exercise those rights.	

Recommendations: No further recommendations at this time.

B Fully Compliant **Evidence:** Online Privacy Notice

Regulation:

(b) The privacy policy shall comply with section 7003, subsections (a) and (b).

Observations/Findings: Thoropass's Privacy Notice complies with the CCPA requirements.

Recommendations: No further recommendations at this time.

C Fully Compliant **Evidence:** Online Privacy Notice

Regulation:

(c) The privacy policy shall be available in a format that allows a consumer to print it out as a document.

Observations/Findings: Thoropass's Privacy Notice is available to print as a document via a link on Thoropass's Privacy Policy Page: <https://thoropass.com/privacy-policy>

Recommendations: No further recommendations at this time.

D Fully Compliant **Evidence:** Online Privacy Notice

Regulation:

(d) The privacy policy shall be posted online and accessible through a conspicuous link that complies with section 7003, subsections (c) and (d), using the word "privacy" on the business's website homepage(s) or on the download or landing page of a mobile application. If the business has a California-specific description of consumers' privacy rights on its website, then the privacy policy shall be included in that description. A business that does not operate a website shall make the privacy policy conspicuously available to consumers. A mobile application may include a link to the privacy policy in the application's settings menu.

Observations/Findings: Thoropass posts its Privacy Notice online through an accessible conspicuous link entitled 'Privacy' on its website homepage located directly here: <https://thoropass.com/privacy-policy/>. Thoropass includes California-specific description of consumers' privacy rights within its Privacy Policy.

Recommendations: No further recommendations at this time.

E Fully Compliant **Evidence:** Online Privacy Notice; Data Protection Agreement (DPA); Subprocessor List

Regulation:

(e) The privacy policy shall include the following information:

(1) A comprehensive description of the business's online and offline information practices, which includes the following:

(A) Identification of the categories of personal information the business has collected about consumers in the preceding 12 months. The categories shall be described using the specific terms set forth in Civil

Code section 1798.140, subdivisions (v)(1)(A) to (K) and (ae)(1) to (2). To the extent that the business has discretion in its description, the business shall describe the category in a manner that provides consumers a meaningful understanding of the information being collected.

(B) Identification of the categories of sources from which the personal information is collected.

(C) Identification of the specific business or commercial purpose for collecting personal information from consumers. The purpose shall be described in a manner that provides consumers a meaningful understanding of why the information is collected.

(D) Identification of the categories of personal information, if any, that the business has sold or shared to third parties in the preceding 12 months. If the business has not sold or shared consumers' personal information in the preceding 12 months, the business shall disclose that fact.

(E) For each category of personal information identified in subsection (e)(1)(D), the categories of third parties to whom the information was sold or shared.

(F) Identification of the specific business or commercial purpose for selling or sharing consumers' personal information. The purpose shall be described in a manner that provides consumers a meaningful understanding of why the information is sold or shared.

(G) A statement regarding whether the business has actual knowledge that it sells or shares the personal information of consumers under 16 years of age.

(H) 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. If the business has not disclosed consumers' personal information for a business purpose in the preceding 12 months, the business shall disclose that fact.

(I) For each category of personal information identified in subsection (e)(1)(H), the categories of third parties to whom the information was disclosed.

(J) Identification of the specific business or commercial purpose for disclosing the consumer's personal information. The purpose shall be described in a manner that provides consumers a meaningful understanding of why the information is disclosed.

(K) A statement regarding whether the business uses or discloses sensitive personal information for purposes other than those specified in section 7027, subsection (m).

(2) An explanation of the rights that the CCPA confers on consumers regarding their personal information, which includes all of 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 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) If the business sells or shares personal information, the right to opt-out of the sale or sharing of their personal information by the business.

(E) If the business uses or discloses sensitive personal information for reasons other than those set forth in section 7027, subsection (m), 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 an employee's, applicant's, or independent contractor's right not to be retaliated against for the exercise of their CCPA rights.

(3) An explanation of how consumers can exercise their CCPA rights and what consumers can expect from that process, which includes all of the following:

(A) An explanation of the methods by which the consumer can exercise their CCPA rights.

(B) Instructions for submitting a request under the CCPA, including any links to an online request form or portal for making such a request, if offered by the business.

(C) If the business sells or shares personal information, and is required to provide a Notice of Right to Opt-out of Sale/Sharing, the contents of the Notice of Right to Opt-out of Sale/Sharing or a link to that

notice in accordance with section 7013, subsection (f).

(D) If the business uses or discloses sensitive personal information for purposes other than those specified in section 7027, subsection (m), and is required to provide a Notice of Right to Limit, the contents of the Notice of Right to Limit or a link to that notice in accordance with section 7014, subsection (f).

(E) A general description of the process the business uses to verify a consumer request to know, request to delete, and request to correct, when applicable, including any information the consumer must provide.

(F) 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.

(G) If the business processes opt-out preference signals in a frictionless manner, information on how consumers can implement opt-out preference signals for the business to process in a frictionless manner.

(H) Instructions on how an authorized agent can make a request under the CCPA on the consumer's behalf.

(I) If the business has actual knowledge that it sells the personal information of consumers under 16 years of age, a description of the processes required by sections 7070 and 7071.

(J) A contact 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.

(4) Date the privacy policy was last updated.

(5) If subject to the data reporting requirements set forth in section 7102, the information required under section 7102, or a link to that information.

Observations/Findings: Thoropass's Privacy Notice contains the following information:

A description of Thoropass's online (and offline) information practices to include:

- Categories of personal information Thoropass has collected about consumers in the last twelve (12) months are described as the following: contact information; demographic and preference data; payment information; content and files; identifiers and device information; geolocation data; and usage data.
- Sources of categories from which personal information is collected, more specifically the consumer and some third-party sources.
- The specific business purpose, in a meaningful manner, for collecting personal information.
- Thoropass does not sell or share any personal information with third parties.
- The categories of personal information disclosed for a business purpose to third parties in the last twelve (12) months.
- The third parties to whom the information was disclosed such as Google and the list of sub-processors provided for here:
<https://trust.thoropass.com/?itemUid=e3fae2ca-94a9-416b-b577-5c90e382df57&source=click>
- The business purpose for which the personal information is disclosed.
- The privacy policy includes a statement regarding limiting the personal information provided to service providers to that which is reasonably necessary for them to perform their functions.

The privacy notice also includes CCPA required information such as the following:

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

- Explanation that a consumer has the right to request that Thoropass disclose what personal information it collects, uses, discloses, and sells.
- Instructions for submitting a verifiable consumer request to know and links to an online request form or portal for making the request, if offered by Thoropass.
- General description of the process Thoropass will use to verify the consumer request, including any information the consumer must provide.
- Identification of the categories of personal information Thoropass has collected about

consumers in the preceding twelve (12) months. The categories will be described in a manner that provides consumers a meaningful understanding of the information being collected.

- Identification of the categories of sources from which the personal information is collected.
- Identification of the business or commercial purpose for collecting or selling personal information. The purpose will be described in a manner that provides consumers a meaningful understanding of why the information is collected or sold.

Disclosure or Sale of Personal Information.

- Thoropass does not sell or disclose personal information.

Right to Request Deletion of Personal Information.

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

Right to Opt-Out of the Sale of Personal Information.

- Thoropass does not sell or disclose personal information.

Right to Non-Discrimination for the Exercise of a Consumer's Privacy Rights.

- Explanation that the consumer has a right not to receive discriminatory treatment by Thoropass for the exercise of the privacy rights conferred by the CCPA.

Authorized Agent.

- Instructions on how an authorized agent can make a request under the CCPA on the consumer's behalf.

Contact for More Information.

- A contact for questions or concerns about Thoropass's privacy policies and practices using a method reflecting the manner in which Thoropass primarily interacts with the consumer.

Date the privacy notice was last updated.

Recommendations: No further recommendations at this time.

7012 Notice at Collection of Personal Information

A Fully Compliant Evidence: Online Privacy Notice

Regulation:

(a) The purpose of the Notice at Collection is to provide consumers with timely notice, at or before the point of collection, about the categories of personal information to be collected from them, the purposes for which the personal information is collected or used, and whether that information is sold or shared, so that consumers have a tool to exercise meaningful control over the business's use of their personal information.

Observations/Findings: Thoropass provides a Privacy Notice at the point of collection providing timely notice about the categories of personal information being collected from them, the purpose of the collection/use, and to advise the consumer their personal information will not be sold or shared. This is intended to provide consumers the information they need to exercise meaningful control over Thoropass's use of their personal information.

Recommendations: No further recommendations at this time.

B Fully Compliant **Evidence:** Online Privacy Notice

Regulation:

(b) The Notice at Collection shall comply with section 7003, subsections (a) and (b).

Observations/Findings: Thoropass's Privacy Notice complies with the CCPA.

Recommendations: No further recommendations at this time.

C Fully Compliant **Evidence:** Online Privacy Notice

Regulation:

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

Observations/Findings: Thoropass's Privacy Notice is made readily available through a conspicuous link entitled "Privacy" on Thoropass's website introduction page and all webpages where personal information is collected.

Recommendations: No further recommendations at this time.

D Fully Compliant **Evidence:** Online Privacy Notice

Regulation:

(d) If a business does not give the Notice at Collection to the consumer at or before the point of collection of their personal information, the business shall not collect personal information from the consumer.

Observations/Findings: Thoropass does not collect any personal information from a consumer without a Privacy Notice being provided to a consumer at the point of collection.

Recommendations: No further recommendations at this time.

E Fully Compliant **Evidence:** Online Privacy Notice

Regulation:

(e) A business shall include the following in its Notice at Collection:

(1) A list of the categories of personal information about consumers, including categories of sensitive personal information, to be collected. Each category of personal information shall be written in a manner that provides consumers a meaningful understanding of the information being collected.

(2) The purpose(s) for which the categories of personal information, including categories of sensitive personal information, are collected and used.

(3) Whether each category of personal information identified in subsection (e)(1) is sold or shared.

(4) The length of time the business intends to retain each category of personal information identified in subsection (e)(1), or if that is not possible, the criteria used to determine the period of time it will be retained.

(5) If the business sells or shares personal information, 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.

Observations/Findings: Thoropass includes the following in its Privacy Notice provided at the point of collection (i.e. Notice at Collection):

- List of categories of personal information including sensitive personal information being collected from the consumer written in an understandable manner.
- Purpose of collection and use of all categories of personal information including sensitive personal information.
- Notification Thoropass doesn't sell or share personal information.
- Thoropass notifies consumers it retains personal information for as long as necessary to provide service and fulfill transactions, comply with legal obligations, resolve disputes, fulfill contract obligations, enforce agreements, and other legitimate/lawful business purposes.
- Thoropass doesn't provide a Notice of Rights to Opt-out of Sale/Sharing since Thoropass doesn't sell/share personal information with third parties.
- Thoropass provides a link to its privacy policy located here:
<https://thoropass.com/privacy-policy/>

Recommendations: No further recommendations at this time.

F Fully Compliant **Evidence:** Online Privacy Notice

Regulation:

(f) If a business collects personal information from a consumer online, the Notice at Collection may be given to the consumer by providing a link that takes the consumer directly to the specific section of the business’s privacy policy that contains the information required in subsection (e)(1) through (6). Directing the consumer to the beginning of the privacy policy, or to another section of the privacy policy that does not contain the required information, so that the consumer is required to scroll through other information in order to determine the categories of personal information to be collected and/or whether the business sells or shares the personal information collected, does not satisfy this standard.

Observations/Findings: Thoropass collects personal information for a consumer online through a form located at: <https://thoropass.com/talk-to-an-expert/> A notice before submitting the information is provided with a link to Thoropass's Privacy Policy. The link takes the consumer directly to the Collection of Personal Information section of the privacy policy detailing the categories of personal information collected and notification Thoropass does not sell or share personal information.

Recommendations: No further recommendations at this time.

G Not Applicable **Evidence:** N/A

Regulation:

(g) Third Parties that Control the Collection of Personal Information. This subsection shall not affect the first party’s obligations under the CCPA to comply with a consumer’s request to opt-out of sale/sharing.
 (1) For purposes of giving Notice at Collection, more than one business may control the collection of a consumer’s personal information, and thus, have an obligation to provide a Notice at Collection in accordance with the CCPA and these regulations.
 (2) A business that, acting as a third party, controls the collection of personal information on another business’s physical premises, such as in a retail store or in a vehicle, shall provide a Notice at Collection in a conspicuous manner at the physical location(s) where it is collecting the personal information.

Observations/Findings: N/A. Thoropass intentionally interacts with a consumer to collect personal information directly from the consumer or is a service provider to other businesses. Thoropass is not considered a third party under CCPA.

Recommendations: Not applicable.

H Not Applicable

Evidence: N/A

Regulation:

(h) A business that neither collects nor controls the collection of personal information directly from the consumer does not need to provide a Notice at Collection to the consumer if it neither sells nor shares the consumer’s personal information.

Observations/Findings: N/A. Thoropass does collect personal information directly from the consumer as identified throughout this assessment.

Recommendations: Not applicable.

I Not Applicable

Evidence: N/A

Regulation:

(i) A data broker registered with the Attorney General pursuant to Civil Code section 1798.99.80 et seq. that collects personal information from a source other than directly from the consumer does not need to provide a Notice at Collection to the consumer if it has included in its registration submission a link to its Online Privacy Notice that includes instructions on how a consumer can submit a request to opt-out of sale/sharing.

Observations/Findings: N/A. Thoropass is not a data broker.

Recommendations: Not applicable.

7013 Notice of Right to Opt-out of Sale/Sharing and the “Do Not Sell or Share My Personal Information” Link

A Not Applicable

Evidence: N/A

Regulation:

(a) The purpose of the Notice of Right to Opt-out of Sale/Sharing is to inform consumers of their right to direct a business that sells or shares their personal information to stop selling or sharing their personal information and to provide them with the opportunity to exercise that right. The purpose of the “Do Not Sell or Share My Personal Information” link is to immediately effectuate the consumer’s right to opt-out of sale/sharing, or in the alternative, direct the consumer to the Notice of Right to Opt-out of Sale/Sharing. Accordingly, clicking the business’s “Do Not Sell or Share My Personal Information” link will either have the immediate effect of opting the consumer out of the sale or sharing of personal information or lead the consumer to a webpage where the consumer can learn about and make that choice.

Observations/Findings: N/A. Thoropass does not sell or share personal information of consumers and is not required to have a Notice of Right to Opt-out of Sale/Sharing.

Recommendations: Not applicable.

B Not Applicable **Evidence:** N/A

Regulation:

(b) The Notice of Right to Opt-out of Sale/Sharing shall comply with section 7003, subsections (a) and (b).

Observations/Findings: N/A. Thoropass does not sell or share personal information of consumers and is not required to have a Notice of Right to Opt-out of Sale/Sharing.

Recommendations: Not applicable.

C Not Applicable **Evidence:** N/A

Regulation:

(c) The “Do Not Sell or Share My Personal Information” link shall be a conspicuous link that complies with section 7003, subsections (c) and (d) and is located at either the header or footer of the business’s internet homepage(s).

Observations/Findings: N/A. Thoropass does not sell or share personal information of consumers and is not required to have a Notice of Right to Opt-out of Sale/Sharing.

Recommendations: Not applicable.

D Not Applicable **Evidence:** N/A

Regulation:

(d) In lieu of posting the “Do Not Sell or Share My Personal Information” link, a business may provide the Alternative Opt-out Link in accordance with section 7015 or process opt-out preference signals in a frictionless manner in accordance with section 7025, subsections (f) and (g). The business must still post a Notice of Right to Opt-out of Sale/Sharing in accordance with these regulations.

Observations/Findings: N/A. Thoropass does not sell or share personal information of consumers and is not required to have a Notice of Right to Opt-out of Sale/Sharing.

Recommendations: Not applicable.

E Not Applicable **Evidence:** N/A

Regulation:

(e) A business that sells or shares the personal information of consumers shall provide the Notice of Right to Opt-out of Sale/Sharing to consumers as follows:

(1) A business shall post the Notice of Right to Opt-out of Sale/Sharing on the internet webpage to which the consumer is directed after clicking on the “Do Not Sell or Share My Personal Information” link. The notice shall include the information specified in subsection (f) or be a link that takes the consumer directly to the specific section of the business’s privacy policy that contains the same information. If clicking on the “Do Not Sell or Share My Personal Information” link immediately effectuates the consumer’s right to opt-out of sale/sharing or if the business processes opt-out

preference signals in a frictionless manner and chooses not to post a link, the business shall provide the notice within its privacy policy.

(2) A business that does not operate a website shall establish, document, and comply with another method by which it informs consumers of their right to opt-out of sale/sharing. That method shall comply with the requirements set forth in section 7003 .

(3) A business shall also provide the notice to opt-out of sale/sharing in the same manner in which it collects the personal information that it sells or shares. Illustrative examples follow.

(A) A business that sells or shares personal information that it collects in the course of interacting with consumers offline, such as in a brick-and-mortar store, shall provide notice through an offline method, e.g., on the paper forms that collect the personal information or by posting signage in the area where the personal information is collected directing consumers to where the notice can be found online.

(B) A business that sells or shares personal information that it collects over the phone shall provide notice orally during the call when the information is collected.

Observations/Findings: N/A. Thoropass does not sell or share personal information of consumers and is not required to have a Notice of Right to Opt-out of Sale/Sharing.

Recommendations: Not applicable.

F Not Applicable

Evidence: N/A

Regulation:

(f) A business shall include the following in its Notice of Right to Opt-out of Sale/Sharing:

(1) A description of the consumer’s right to opt-out of the sale or sharing of their personal information by the business; and

(2) Instructions on how the consumer can submit a request to opt-out of sale/sharing. If notice is provided online, the notice shall include the interactive form by which the consumer can submit their request to opt-out of sale/sharing online, as required by section 7026, subsection (a)(1). If the business does not operate a website, the notice shall explain the offline method by which the consumer can submit their request to opt-out of sale/sharing.

Observations/Findings: N/A. Thoropass does not sell or share personal information of consumers and is not required to have a Notice of Right to Opt-out of Sale/Sharing.

Recommendations: Not applicable.

G Fully Compliant

Evidence: Online Privacy Notice

Regulation:

(g) A business does not need to provide a Notice of Right to Opt-out of Sale/Sharing or the “Do Not Sell or Share My Personal Information” link if:

(1) It does not sell or share personal information; and

(2) It states in its privacy policy that it does not sell or share personal information.

Observations/Findings: Thoropass does not sell or share personal information of consumers and is not required to have a Notice of Right to Opt-out of Sale/Sharing.

Recommendations: No further recommendations at this time.

H Fully Compliant

Evidence: Online Privacy Notice

Regulation:

(h) A business shall not sell or share the personal information it collected during the time the business did not have a Notice of Right to Opt-out of Sale/Sharing posted unless it obtains the consent of the consumer.

Observations/Findings: Thoropass does not sell or share personal information of consumers and is not required to have a Notice of Right to Opt-out of Sale/Sharing.

Recommendations: No further recommendations at this time.

7014 Notice of Right to Limit and the “Limit the Use of My Sensitive Personal Information” Link

A Not Applicable

Evidence: N/A

Regulation:

(a) The purpose of the Notice of Right to Limit is to inform consumers of their right to limit a business’s use and disclosure of their sensitive personal information and to provide them with the opportunity to exercise that right. The purpose of the “Limit the Use of My Sensitive Personal Information” link is to immediately effectuate the consumer’s right to limit, or in the alternative, direct the consumer to the Notice of Right to Limit. Accordingly, clicking the business’s “Limit the Use of My Sensitive Personal Information” link will either have the immediate effect of limiting the use and disclosure of the consumer’s sensitive personal information or lead the consumer to a webpage where the consumer can learn about and make that choice.

Observations/Findings: N/A. Thoropass only uses or discloses sensitive personal information for the following purposes under reasonably necessary use/disclosure and proportionate purposes, which exempts Thoropass from the requirement to post a Notice of Right to Limit:

- To perform Thoropass's services or provide the Thoropass's product reasonably expected by an average consumer who requests these goods or services.
- To prevent, detect, and investigate security incidents compromising the availability, authenticity, integrity, or confidentiality of stored/transmitted personal information.
- To resist malicious, deceptive, fraudulent, or illegal actions directed at Thoropass and to prosecute those responsible for those actions.
- To ensure the physical safety of natural persons.
- For short-term, transient use, include, but not limited to, non-personalized advertising shown as part of a consumer's current interaction with Thoropass, provided: Thoropass does not disclose personal information to another third party; does not use this personal information to build a profile about the consumer; or otherwise alter the consumer's experience outside the current interaction with Thoropass.
- To perform services on behalf of Thoropass.
- To verify or maintain the quality or safety of Thoropass's products or services and to improve, upgrade, or enhance the product or service.
- To collect or process sensitive personal information where the collection/processing is not for the purpose of inferring characteristics about a consumer.

Recommendations: Not applicable.

B Not Applicable

Evidence: N/A

Regulation:

(b) The Notice of Right to Limit shall comply with section 7003, subsections (a) and (b).

Observations/Findings: N/A. Thoropass is exempt from posting a Notice of Right to Limit.

Recommendations: Not applicable.

C Not Applicable

Evidence: N/A

Regulation:

(c) The “Limit the Use of My Sensitive Personal Information” link shall be a conspicuous link that complies with section 7003, subsections (c) and (d), and is located at either the header or footer of the business’s internet homepage(s).

Observations/Findings: N/A. Thoropass is exempt from posting a Notice of Right to Limit.

Recommendations: Not applicable.

D Not Applicable

Evidence: N/A

Regulation:

(d) In lieu of posting the “Limit the Use of My Sensitive Personal Information” link, a business may provide the Alternative Opt-out Link in accordance with section 7015. The business shall still post a Notice of Right to Limit in accordance with these regulations.

Observations/Findings: N/A. Thoropass is exempt from posting a Notice of Right to Limit.

Recommendations: Not applicable.

E Not Applicable

Evidence: N/A

Regulation:

(e) A business that uses or discloses a consumer’s sensitive personal information for purposes other than those specified in section 7027, subsection (m), shall provide the Notice of Right to Limit to consumers as follows:

(1) A business shall post the Notice of Right to Limit on the internet webpage to which the consumer is directed after clicking on the “Limit the Use of My Sensitive Personal Information” link. The notice shall include the information specified in subsection (f) or be a link that takes the consumer directly to the specific section of the business’s privacy policy that contains the same information. If clicking on the “Limit the Use of My Sensitive Personal Information” link immediately effectuates the consumer’s right to limit, the business shall provide the notice within its privacy policy.

(2) A business that does not operate a website shall establish, document, and comply with another method by which it informs consumers of their right to limit. That method shall comply with the requirements set forth in section 7003.

Observations/Findings: N/A. Thoropass only uses or discloses sensitive personal information for the following purposes under reasonably necessary use/disclosure and proportionate purposes, which exempts Thoropass from the requirement to post a Notice of Right to Limit:

- To perform Thoropass's services or provide the Thoropass's product reasonably expected by an average consumer who requests these goods or services.
- To prevent, detect, and investigate security incidents compromising the availability, authenticity,

<p>integrity, or confidentiality of stored/transmitted personal information.</p> <ul style="list-style-type: none"> ● To resist malicious, deceptive, fraudulent, or illegal actions directed at Thoropass and to prosecute those responsible for those actions. ● To ensure the physical safety of natural persons. ● For short-term, transient use, include, but not limited to, non-personalized advertising shown as part of a consumer's current interaction with Thoropass, provided: Thoropass does not disclose personal information to another third party; does not use this personal information to build a profile about the consumer; or otherwise alter the consumer's experience outside the current interaction with Thoropass. ● To perform services on behalf of Thoropass. ● To verify or maintain the quality or safety of Thoropass's products or services and to improve, upgrade, or enhance the product or service. ● To collect or process sensitive personal information where the collection/processing is not for the purpose of inferring characteristics about a consumer.
<p>Recommendations: Not applicable.</p>

F Not Applicable	Evidence: N/A
<p>Regulation: (f) A business shall include the following in its Notice of Right to Limit: (1) A description of the consumer's right to limit; and (2) Instructions on how the consumer can submit a request to limit. If notice is provided online, the notice shall include the interactive form by which the consumer can submit their request to limit online, as required by section 7027, subsection (b)(1). If the business does not operate a website, the notice shall explain the offline method by which the consumer can submit their request to limit.</p>	
<p>Observations/Findings: N/A. Thoropass is exempt from posting a Notice of Right to Limit.</p>	
<p>Recommendations: Not applicable.</p>	

G Fully Compliant	Evidence: Online Privacy Notice; PT-02 Authority to Process PII
<p>Regulation: (g) A business does not need to provide a Notice of Right to Limit or the "Limit the Use of My Sensitive Personal Information" link if: (1) It only uses and discloses sensitive personal information that it collected about the consumer for the purposes specified in section 7027, subsection (m), and states so in its privacy policy; or (2) It only collects or processes sensitive personal information without the purpose of inferring characteristics about a consumer, and states so in its privacy policy.</p>	
<p>Observations/Findings: Thoropass's Privacy Policy contains the following related to disclosure of personal information:</p> <ul style="list-style-type: none"> ● Thoropass will disclose personal information to third parties with consent or as necessary to complete a transaction or provide services the consumer requested or authorized. ● Thoropass may share each category identified in the privacy policy for the following business purposes: <ul style="list-style-type: none"> ○ To third-party service providers such as data storage, processing facilities, vendors, and/or consultants assisting Thoropass in its work. Personal information is limited to only what is reasonably necessary. ○ To law enforcement or other government agencies if legally required or in Thoropass's interest to protect property, legal rights, or safety of others. 	

- As part of any merger, acquisition, debt financing, sale of company assets, or similar transaction as well as in the event of insolvency, bankruptcy, or receivership.
- To better understand how Thoropass's services are used.
- Share de-identified information according to applicable law.

Recommendations: No further recommendations at this time.

H Fully Compliant

Evidence: Online Privacy Notice; PT-02 Authority to Process PII

Regulation:

(h) A business shall not use or disclose sensitive personal information it collected during the time the business did not have a Notice of Right to Limit posted for purposes other than those specified in section 7027, subsection (m), unless it obtains the consent of the consumer.

Observations/Findings: Thoropass does not use or disclose sensitive personal information without a Notice of Right to Limit posted except as identified above.

Recommendations: No further recommendations at this time.

7015 Alternative Opt-out Link

A Not Applicable

Evidence: N/A

Regulation:

(a) The purpose of the Alternative Opt-out Link is to provide businesses the option of providing consumers with a single, clearly-labeled link that allows consumers to easily exercise both their right to opt-out of sale/sharing and right to limit, instead of posting the two separate “Do Not Sell or Share My Personal Information” and “Limit the Use of My Sensitive Personal Information” links. The Alternative Opt-out Link shall direct the consumer to a webpage that informs them of both their right to opt-out of sale/sharing and right to limit and provides them with the opportunity to exercise both rights.

Observations/Findings: N/A. Thoropass doesn't utilize the Alternative Opt-out Link since Thoropass does not sell or share personal information and is not required to have a Notice of Right to Limit.

Recommendations: Not applicable.

B Not Applicable

Evidence: N/A

Regulation:

(b) A business that chooses to use an Alternative Opt-out Link shall title the link, “Your Privacy Choices,” or, “Your California Privacy Choices,” and shall include the following opt-out icon adjacent to the title. The link shall be a conspicuous link that complies with section 7003, subsections (c) and (d), and is located at either the header or footer of the business’s internet homepage(s). The icon shall be approximately the same size as other icons used by the business in the header or footer of its webpage.

Observations/Findings: N/A. Thoropass doesn't utilize the Alternative Opt-out Link since Thoropass does not sell or share personal information and is not required to have a Notice of Right to Limit.

Recommendations: Not applicable.

C Not Applicable **Evidence:** N/A

Regulation:

(c) The Alternative Opt-out Link shall direct the consumer to a webpage that includes the following information:

(1) A description of the consumer’s right to opt-out of sale/sharing and right to limit, which shall comply with section 7003, subsections (a) and (b); and

(2) The interactive form or mechanism by which the consumer can submit their request to opt-out of sale/sharing and their right to limit online. The method shall be easy for consumers to execute, shall require minimal steps, and shall comply with section 7004.

Observations/Findings: N/A. Thoropass doesn't utilize the Alternative Opt-out Link since Thoropass does not sell or share personal information and is not required to have a Notice of Right to Limit.

Recommendations: Not applicable.

7016 Notice of Financial Incentive

A Not Applicable **Evidence:** N/A

Regulation:

(a) The purpose of the Notice of Financial Incentive is to explain to the consumer the material terms of a financial incentive or price or service difference the business is offering so that the consumer may make an informed decision about whether to participate. A business that does not offer a financial incentive or price or service difference is not required to provide a Notice of Financial Incentive.

Observations/Findings: N/A. Thoropass does not offer a financial incentive or price/service difference and is not required to provide a Notice of Financial Incentive.

Recommendations: Not applicable.

B Not Applicable **Evidence:** N/A

Regulation:

(b) The Notice of Financial Incentive shall comply with section 7003, subsections (a) and (b).

Observations/Findings: N/A. Thoropass does not offer a financial incentive or price/service difference and is not required to provide a Notice of Financial Incentive.

Recommendations: Not applicable.

C Not Applicable **Evidence:** N/A

Regulation:

(c) The Notice of Financial Incentive shall be readily available where consumers will encounter it before opting-in to the financial incentive or price or service difference. If the business offers the

financial incentive or price or service difference online, the notice may be given by providing a link that takes the consumer directly to the specific section of a business's privacy policy that contains the information required in subsection (d).

Observations/Findings: N/A. Thoropass does not offer a financial incentive or price/service difference and is not required to provide a Notice of Financial Incentive.

Recommendations: Not applicable.

D Not Applicable

Evidence: N/A

Regulation:

- (d) A business shall include the following in its Notice of Financial Incentive:
- (1) A succinct summary of the financial incentive or price or service difference offered;
 - (2) A description of the material terms of the financial incentive or price or service difference, including the categories of personal information that are implicated by the financial incentive or price or service difference and the value of the consumer's data;
 - (3) How the consumer can opt-in to the financial incentive or price or service difference;
 - (4) A statement of the consumer's right to withdraw from the financial incentive at any time and how the consumer may exercise that right; and
 - (5) An explanation of how the price or service difference is reasonably related to the value of the consumer's data, including:
 - (A) A good-faith estimate of the value of the consumer's data that forms the basis for offering the price or service difference; and
 - (B) A description of the method(s) the business used to calculate the value of the consumer's data.

Observations/Findings: N/A. Thoropass does not offer a financial incentive or price/service difference and is not required to provide a Notice of Financial Incentive.

Recommendations: Not applicable.

Article 3 Business Practices for Handling Consumer Requests

7020 Methods for Submitting Requests to Delete, Requests to Correct, and Requests to Know

A Fully Compliant

Evidence: Online Privacy Notice

Regulation:

- (a) A business that operates exclusively online and has a direct relationship with a consumer from whom it collects personal information shall only be required to provide an email address for submitting requests to delete, requests to correct, and requests to know.

Observations/Findings: Thoropass exclusively operates online and has direct relationships with consumers from whom it collects personal information. Thoropass includes an email at privacy@thoropass.com for consumers to submit requests to delete, requests to correct, and requests to know.

Note: Thoropass has not received any CCPA related requests from any consumers over the last

twelve (12) months.

Recommendations: No further recommendations at this time.

B Not Applicable

Evidence: N/A

Regulation:

(b) A business that does not fit the description in subsection (a) shall provide two or more designated methods for submitting requests to delete, requests to correct, and requests to know. One of those methods must be a toll-free telephone number. If the business maintains an internet website, one of the methods for submitting these requests shall be through its website, such as through a webform. Other methods for submitting requests to delete, requests to correct, and requests to know may include, but are not limited to, a designated email address, a form submitted in person, and a form submitted through the mail.

Observations/Findings: N/A. Thoropass exclusively operates online and has direct relationships with consumers from whom it collects personal information. Thoropass includes an email at privacy@thoropass.com for consumers to submit requests to delete, requests to correct, and requests to know.

Recommendations: Not applicable.

C Fully Compliant

Evidence: PT-02 Authority to Process PII

Regulation:

(c) A business shall consider the methods by which it primarily interacts with consumers when determining which methods to provide for submitting requests to delete, requests to correct, and requests to know. If the business interacts with consumers in person, the business shall consider providing an in-person method such as a printed form the consumer can directly submit or send by mail, a tablet or computer portal that allows the consumer to complete and submit an online form, or a telephone with which the consumer can call the business's toll-free number.

Observations/Findings: Thoropass exclusively operates online and has direct relationships with consumers from whom it collects personal information. Thoropass includes an email at privacy@thoropass.com for consumers to submit requests to delete, requests to correct, and requests to know.

Note: Thoropass has not received any CCPA related requests from any consumers over the last twelve (12) months.

Recommendations: No further recommendations at this time.

D Fully Compliant

Evidence: PT-02 Authority to Process PII

Regulation:

(d) A business may use a two-step process for online requests to delete where the consumer must first, submit the request to delete and then second, separately confirm that they want their personal information deleted provided that the business otherwise complies with section 7004.

Observations/Findings: Thoropass utilizes a two-step process for requests to delete where the consumer first submits a request to delete and then separately confirms with the consumer they want

their personal information deleted.

Note: Thoropass has not received any CCPA related requests from any consumers over the last twelve (12) months.

Recommendations: No further recommendations at this time.

E Fully Compliant

Evidence: PT-02 Authority to Process PII

Regulation:

(e) If a consumer submits a request in a manner that is not one of the designated methods of submission, or is deficient in some manner unrelated to the verification process, the business shall either:

- (1) Treat the request as if it had been submitted in accordance with the business's designated manner, or
- (2) Provide the consumer with information on how to submit the request or remedy any deficiencies with the request, if applicable.

Observations/Findings: If a consumer submits a request in a manner outside of utilizing email to privacy@thoropass.com or if the request is deficient in some manner unrelated to verification, Thoropass will either treat the request as if submitted in the designated method or provide the consumer additional information on how to submit the request (or remedy any deficiencies).

Note: Thoropass has not received any CCPA related requests from any consumers over the last twelve (12) months.

Recommendations: No further recommendations at this time.

7021 Timelines for Responding to Requests to Delete, Requests to Correct, and Requests to Know

A Fully Compliant

Evidence: PT-02 Authority to Process PII

Regulation:

(a) No later than 10 business days after receiving a request to delete, request to correct, or request to know, a business shall confirm receipt of the request and provide information about how the business will process the request. The information provided shall describe in general the business's verification process and when the consumer should expect a response, except in instances where the business has already granted or denied the request. The confirmation may be given in the same manner in which the request was received.

Observations/Findings: Thoropass will confirm receipt of a request to delete, correct, or know no later than ten (10) days after receiving the request. Thoropass will provide information on Thoropass's verification process and when the consumer should expect a response, except in instances where Thoropass has already granted or denied the request. The confirmation will be made through email, the same designated manner the request was made.

Note: Thoropass has not received any CCPA related requests from any consumers over the last twelve (12) months.

Recommendations: Not applicable.

B Fully Compliant

Evidence: PT-02 Authority to Process PII

Regulation:

(b) Businesses shall respond to a request to delete, request to correct, and request to know no later than 45 calendar days after receipt of the request. The 45- day period will begin on the day that the business receives the request, regardless of time required to verify the request. If the business cannot verify the consumer within the 45-day time period, the business may deny the request. If necessary, businesses may take up to an additional 45 calendar days to respond to the consumer’s request, for a maximum total of 90 calendar days from the day the request is received, provided that the business provides the consumer with notice and an explanation of the reason that the business will take more than 45 days to respond to the request.

Observations/Findings: Thoropass will respond to a request to delete, correct, or know no later than forty-five (45) calendar days after receipt of the request. Note: The forty-five (45) day period begins on the day Thoropass receives the request, regardless of time required to verify the request. If Thoropass cannot verify the consumer within the forty-five (45) day time period, Thoropass may deny the request. Thoropass may take up to an additional forty-five (45) calendar days to respond to a consumer's request (for a maximum of ninety (90) calendar days from the day the request is received) provided Thoropass notifies the consumer with an explanation.

Note: Thoropass has not received any CCPA related requests from any consumers over the last twelve (12) months.

Recommendations: No further recommendations at this time.

7022 Requests to Delete

A Fully Compliant Evidence: PT-02 Authority to Process PII

Regulation:

(a) For requests to delete, if a business cannot verify the identity of the requestor pursuant to the regulations set forth in Article 5, the business may deny the request to delete. The business shall inform the requestor that their identity cannot be verified.

Observations/Findings: If Thoropass cannot verify the identity of a requestor making a request to delete pursuant to Article 5 below, Thoropass may deny the request and inform the requestor their identity cannot be verified.

Note: Thoropass has not received any CCPA related requests from any consumers over the last twelve (12) months.

Recommendations: No further recommendations at this time.

B Fully Compliant Evidence: PT-02 Authority to Process PII

Regulation:

(b) A business shall comply with a consumer’s request to delete their personal information by:

- (1) Permanently and completely erasing the personal information from its existing systems except archived or backup systems, deidentifying the personal information, or aggregating the consumer information;
- (2) Notifying the business’s service providers or contractors of the need to delete from their records the consumer’s personal information that they collected pursuant to their written contract with the business, or if enabled to do so by the service provider or contractor, the business shall delete the personal information that the service provider or contractor collected pursuant to their written contract with the business; and
- (3) Notifying all third parties to whom the business has sold or shared the personal information of the

need to delete the consumer's personal information unless this proves impossible or involves disproportionate effort. If a business claims that notifying some or all third parties would be impossible or would involve disproportionate effort, the business shall provide the consumer a detailed explanation that includes enough facts to give a consumer a meaningful understanding as to why the business cannot notify all third parties. The business shall not simply state that notifying all third parties is impossible or would require disproportionate effort.

Observations/Findings: Thoropass will comply with a consumer's request to delete their personal information by:

- Permanently and completely erasing the personal information for systems (except archived/backup systems), deidentifying the personal information, or aggregating the consumer information.
- Notify service providers/contractors to delete the record of the consumer's personal information or if enabled, Thoropass will delete the personal information the service provider/contractor collected as per contract.
- Since Thoropass doesn't sell or share personal information with third parties, Thoropass will not need to notify any third parties on a request to delete.

Note: Thoropass has not received any CCPA related requests from any consumers over the last twelve (12) months.

Recommendations: No further recommendations at this time.

C Fully Compliant

Evidence: PT-02 Authority to Process PII

Regulation:

(c) A service provider or contractor shall, with respect to personal information that they collected pursuant to their written contract with the business and upon notification by the business, cooperate with the business in responding to a request to delete by doing all of the following:

- (1) Permanently and completely erasing the personal information from its existing systems except archived or backup systems, deidentifying the personal information, aggregating the consumer information, or enabling the business to do so.
- (2) To the extent that an exception applies to the deletion of personal information, deleting or enabling the business to delete the consumer's personal information that is not subject to the exception and refraining from using the consumer's personal information retained for any purpose other than the purpose provided for by that exception.
- (3) Notifying any of its own service providers or contractors of the need to delete from their records in the same manner the consumer's personal information that they collected pursuant to their written contract with the service provider or contractor.
- (4) Notifying any other service providers, contractors, or third parties that may have accessed personal information from or through the service provider or contractor, unless the information was accessed at the direction of the business, of the need to delete the consumer's personal information unless this proves impossible or involves disproportionate effort.

Observations/Findings: Thoropass's service providers or contractors, accordingly to contract, will do the following in respect to a request to delete personal information:

- Permanently and completely erasing the personal information for systems (except archived/backup systems), deidentifying the personal information, or aggregating the consumer information.
- Delete personal information not subject to any exception and refrain from using the consumer's personal information retained for any purpose other than the purpose provided by the exception.
- Notify service providers/contractors to delete the record of the consumer's personal information or if enabled, Thoropass will delete the personal information the service provider/contractor

collected as per contract.

- Notify any other service providers, contractors, or third parties having accessed personal information from the service provider/contractor (unless the information was accessed at the direction of Thoropass) of the need to delete consumer's personal information (unless proven to be impossible or involves disproportionate effort).

Thoropass as a service provider or contractor will:

- Permanently and completely erasing the personal information for systems (except archived/backup systems), deidentifying the personal information, or aggregating the consumer information.
- Delete personal information not subject to any exception and refrain from using the consumer's personal information retained for any purpose other than the purpose provided by the exception.
- Notify service providers/contractors to delete the record of the consumer's personal information or if enabled, Thoropass will delete the personal information the service provider/contractor collected as per contract.
- Notify any other service providers, contractors, or third parties having accessed personal information from the service provider/contractor (unless the information was accessed at the direction of Thoropass) of the need to delete consumer's personal information (unless proven to be impossible or involves disproportionate effort).

Note: Thoropass has not received any CCPA related requests from any consumers over the last twelve (12) months.

Recommendations: No further recommendations at this time.

D Fully Compliant

Evidence: PT-02 Authority to Process PII

Regulation:

(d) If a business, service provider, or contractor stores any personal information on archived or backup systems, it may delay compliance with the consumer's request to delete, with respect to data stored on the archived or backup system, until the archived or backup system relating to that data is restored to an active system or is next accessed or used for a sale, disclosure, or commercial purpose.

Observations/Findings: If Thoropass, a service provider, or a contractor stores any personal information on archived/backup systems, it may delay compliance with a request to delete with respect to state stored on the archived/backup system until the system related to the data is restored to an active state (or is next accessed or used for sale, disclosure, or commercial purposes).

Recommendations: No further recommendations at this time.

E Fully Compliant

Evidence: PT-02 Authority to Process PII; 00C Data Retention Schedule

Regulation:

(e) In responding to a request to delete, a business shall inform the consumer whether it has complied with the consumer's request. The business shall also inform the consumer that it will maintain a record of the request as required by section 7101, subsection (a). A business, service provider, contractor, or third party may retain a record of the request for the purpose of ensuring that the consumer's personal information remains deleted from its records.

Observations/Findings: In responding to a request, Thoropass will inform the consumer whether it has complied with the request and will maintain a record of the request for at least twenty-four (24) months. *Note: Thoropass, its service provider, its contractor, or its third party may retain a record of*

the request for the purpose of ensuring the consumer's personal information remains deleted from its records.

Recommendations: No further recommendations at this time.

F Fully Compliant

Evidence: PT-02 Authority to Process PII

Regulation:

(f) In cases where a business denies a consumer's request to delete in whole or in part, the business shall do all of the following:

- (1) Provide to the consumer a detailed explanation of the basis for the denial, including any conflict with federal or state law, exception to the CCPA, or factual basis for contending that compliance would be impossible or involve disproportionate effort, unless prohibited from doing so by law;.
- (2) Delete the consumer's personal information that is not subject to the exception.
- (3) Not use the consumer's personal information retained for any other purpose than provided for by that exception.; and
- (4) Instruct its service providers and contractors to delete the consumer's personal information that is not subject to the exception and to not use the consumer's personal information retained for any purpose other than the purpose provided for by that exception.

Observations/Findings: If Thoropass denies the request to delete, Thoropass will:

- Inform the consumer that it will not comply with the consumer's request and describe the basis for the denial, including any conflict with federal or state law, or exception to the CCPA, unless prohibited from doing so by law;
- Delete the consumer's personal information that is not subject to the exception;
- Not use the consumer's personal information retained for any other purpose than provided for by that exception; and
- Instruct service providers and contractors to delete the consumer's personal information not subject to an exception and to not use the consumer's personal information retained for any purpose other than the purpose provided for by the exception.

Note: Thoropass has not received any CCPA related requests from any consumers over the last twelve (12) months.

Recommendations: No further recommendations at this time.

G Not Applicable

Evidence: N/A

Regulation:

(g) If a business that denies a consumer's request to delete sells or shares personal information and the consumer has not already made a request to opt-out of sale/sharing, the business shall ask the consumer if they would like to opt-out of the sale or sharing of their personal information and shall include either the contents of, or a link to, the Notice of Right to Opt-out of Sale/Sharing in accordance with section 7013.

Observations/Findings: N/A. Thoropass does not sell or share personal information.

Recommendations: Not applicable.

H Not Applicable

Evidence: N/A

Regulation:

(h) In responding to a request to delete, a business may present the consumer with the choice to delete select portions of their personal information as long as a single option to delete all personal information is also offered. A business that provides consumers the ability to delete select categories of personal information in other contexts (e.g., purchase history, browsing history, voice recordings), however, must inform consumers of their ability to do so and direct them to how they can do so.

Observations/Findings: N/A. Thoropass does not offer the choice to delete select portions of their personal information.

Recommendations: Not applicable.

7023 Requests to Correct

A Fully Compliant

Evidence: PT-02 Authority to Process PII

Regulation:

(a) For requests to correct, if a business cannot verify the identity of the requestor pursuant to the regulations set forth in Article 5, the business may deny the request to correct. The business shall inform the requestor that their identity cannot be verified.

Observations/Findings: Thoropass may deny an individual access to or a request to change their personally identifiable information based on the inability to verify the identity of the requestor or regulatory requirements and will inform the individual of the denial along with the reason for the denial in a timely manner, unless prohibited by regulations.

Note: Thoropass has not received any CCPA related requests from any consumers over the last twelve (12) months.

Recommendations: No further recommendations at this time.

B Fully Compliant

Evidence: PT-02 Authority to Process PII

Regulation:

(b) In determining the accuracy of the personal information that is the subject of a consumer's request to correct, the business shall consider the totality of the circumstances relating to the contested personal information. A business may deny a consumer's request to correct if it determines that the contested personal information is more likely than not accurate based on the totality of the circumstances.

(1) Considering the totality of the circumstances includes, but is not limited to, considering:

(A) The nature of the personal information (e.g., whether it is objective, subjective, unstructured, sensitive, etc.).

(B) How the business obtained the contested information.

(C) Documentation relating to the accuracy of the information whether provided by the consumer, the business, or another source. Requirements regarding documentation are set forth in subsection (d).

(2) If the business is not the source of the personal information and has no documentation in support of the accuracy of the information, the consumer's assertion of inaccuracy may be sufficient to establish that the personal information is inaccurate.

Observations/Findings: In determining the accuracy of the personal information subject to a consumer's request to correct, Thoropass will consider the totality of the circumstances related to the

contested personal information. Thoropass may deny a consumer's request to correct if it determines the contested personal information is more likely than not accurate based on the totality of the circumstances. Thoropass will consider the following:

- Nature of the personal information (such as whether it is objective, subjective, unstructured, sensitive, or other);
- How Thoropass obtained the information;
- Any documentation relating to the accuracy of the information (whether provided by the consumer, Thoropass, or another source).
- If Thoropass is not the source of personal information and has no documentation to support the accuracy of the information, the consumer's assertion of inaccuracy may be sufficient to establish the personal information is inaccurate.

Note: Thoropass has not received any CCPA related requests from any consumers over the last twelve (12) months.

Recommendations: No further recommendations at this time.

C Fully Compliant Evidence: PT-02 Authority to Process PII

Regulation:

(c) A business that complies with a consumer's request to correct shall correct the personal information at issue on its existing systems. The business shall also instruct all service providers and contractors that maintain the personal information at issue pursuant to their written contract with the business to make the necessary corrections in their respective systems. Service providers and contractors shall comply with the business's instructions to correct the personal information or enable the business to make the corrections. If a business, service provider, or contractor stores any personal information that is the subject of the request to correct on archived or backup systems, it may delay compliance with the consumer's request to correct, with respect to data stored on the archived or backup system, until the archived or backup system relating to that data is restored to an active system or is next accessed or used.

Observations/Findings: Thoropass will also instruct all service providers and contractors maintaining the personal information at issue to make the necessary corrections in their respective systems. Service providers and contractors should comply with Thoropass's instructions to correct the information as per agreements.

If Thoropass, its service provider, or its contractor stores any personal information on archived/backup systems, it may delay compliance with a request to delete with respect to state stored on the archived/backup system until the system related to the data is restored to an active state (or is next accessed or used for sale, disclosure, or commercial purposes).

Recommendations: No further recommendations at this time.

D Fully Compliant Evidence: PT-02 Authority to Process PII

Regulation:

(d) Documentation.

(1) A business shall accept, review, and consider any documentation that the consumer provides in connection with their right to correct whether provided voluntarily or as required by the business. Consumers should make a good-faith effort to provide businesses with all necessary information available at the time of the request.

(2) A business may require the consumer to provide documentation if necessary to rebut its own

documentation that the personal information is accurate. In determining the necessity of the documentation requested, the business shall consider the following:

- (A) The nature of the personal information at issue (e.g., whether it is objective, subjective, unstructured, sensitive, etc.).
- (B) The nature of the documentation upon which the business considers the personal information to be accurate (e.g., whether the documentation is from a trusted source, whether the documentation is verifiable, etc.)
- (C) The purpose for which the business collects, maintains, or uses the personal information.
- (D) The impact on the consumer.

(3) Any documentation provided by the consumer in connection with their request to correct shall only be used and/or maintained by the business for the purpose of correcting the consumer's personal information and to comply with the record-keeping obligations under section 7101.

(4) The business shall implement and maintain reasonable security procedures and practices in maintaining any documentation relating to the consumer's request to correct.

Observations/Findings: As it relates to documentation, Thoropass will accept, review, and consider any documentation the consumer provides in connection with their right to correct whether provided voluntarily or as required by Thoropass. Consumers should make a good-faith effort to provide Thoropass with all necessary information available at the time of the request. Thoropass may require consumers to provide documentation, if necessary, to rebut its own documentation regarding the accuracy of personal information. In determine the necessity of the documentation requested, Thoropass will consider the following:

- Nature of the personal information at issue (whether it is objective, subjective, unstructured, sensitive, or other).
- Nature of the documentation upon which Thoropass considers the personal information to be accurate (whether the documentation is from trusted sources, verifiable, or other).
- Purpose for which Thoropass collected, maintained, or used the personal information.

Impact to the consumer: Any documentation provided by the consumer in connection with their request to correct will only be used/maintained by Thoropass for the purpose of correction and to comply with record-keeping obligations.

Thoropass will implement and maintain reasonable security processes in maintaining any documentation related to a consumer's request to correct. *Note: Thoropass has not received any CCPA related requests from any consumers over the last twelve (12) months.*

Recommendations: No further recommendations at this time.

E Fully Compliant **Evidence:** PT-02 Authority to Process PII

Regulation:

(e) A business may delete the contested personal information as an alternative to correcting the information if the deletion of the personal information does not negatively impact the consumer, or the consumer consents to the deletion.

Observations/Findings: Thoropass may delete the contested personal information as an alternative to correcting the information if the deletion of the personal information does not negatively impact the consumer or the consumer consents to the deletion.

Recommendations: No further recommendations at this time.

F Fully Compliant

Evidence: PT-02 Authority to Process PII

Regulation:

(f) In responding to a request to correct, a business shall inform the consumer whether it has complied with the consumer's request. If the business denies a consumer's request to correct in whole or in part, the business shall do the following:

(1) Explain the basis for the denial, including any conflict with federal or state law, exception to the CCPA, inadequacy in the required documentation, or contention that compliance proves impossible or involves disproportionate effort.

(2) If a business claims that complying with the consumer's request to correct would be impossible or would involve disproportionate effort, the business shall provide the consumer a detailed explanation that includes enough facts to give a consumer a meaningful understanding as to why the business cannot comply with the request. The business shall not simply state that it is impossible or would require disproportionate effort.

Observations/Findings: Thoropass will inform the consumer whether it has complied with the consumer's request. Thoropass may deny an individual access to or a request to change their personally identifiable information based on the inability to verify the identity of the requestor or regulatory requirements and will inform the individual of the denial along with the reason for the denial in a timely manner, unless prohibited by regulations. *Note: Thoropass has not received any CCPA related requests from any consumers over the last twelve (12) months.*

Recommendations: No further recommendations at this time.

G Fully Compliant

Evidence: PT-02 Authority to Process PII

Regulation:

(g) A business may deny a consumer's request to correct if the business has denied the consumer's request to correct the same alleged inaccuracy within the past six months of receiving the request. However, the business must treat the request to correct as new if the consumer provides new or additional documentation to prove that the information at issue is inaccurate.

Observations/Findings: Thoropass may deny a consumer's request to correct if Thoropass has denied the consumer's request to correct the same alleged inaccuracy within the past six (6) months of receiving the request; however, Thoropass will treat the request as new if the consumer provides new/additional documentation to prove the information inaccurate. *Note: Thoropass has not received any CCPA related requests from any consumers over the last twelve (12) months.*

Recommendations: No further recommendations at this time.

H Fully Compliant

Evidence: PT-02 Authority to Process PII

Regulation:

(h) A business may deny a request to correct if it has a good-faith, reasonable, and documented belief that a request to correct is fraudulent or abusive. The business shall inform the requestor that it will not comply with the request and shall provide an explanation why it believes the request is fraudulent or abusive.

Observations/Findings: Thoropass may deny a consumer's request to correct if Thoropass has denied the consumer's request to correct the same alleged inaccuracy within the past six (6) months of receiving the request; however, Thoropass will treat the request as new if the consumer provides new/additional documentation to prove the information inaccurate. *Note: Thoropass has not received*

any CCPA related requests from any consumers over the last twelve (12) months.

Recommendations: No further recommendations at this time.

I Fully Compliant

Evidence: PT-02 Authority to Process PII

Regulation:

(i) Where the business is not the source of the information that the consumer contends is inaccurate, in addition to processing the consumer's request, the business may provide the consumer with the name of the source from which the business received the alleged inaccurate information.

Observations/Findings: Where Thoropass is not the source of the contended information, in addition to processing the request to correct, Thoropass may provide the consumer with the name of the source from which Thoropass received the alleged inaccurate information. *Note: Thoropass has not received any CCPA related requests from any consumers over the last twelve (12) months.*

Recommendations: No further recommendations at this time.

J Fully Compliant

Evidence: PT-02 Authority to Process PII

Regulation:

(j) Upon request, a business shall disclose specific pieces of personal information that the business maintains and has collected about the consumer to allow the consumer to confirm that the business has corrected the inaccurate information that was the subject of the consumer's request to correct. This disclosure shall not be considered a response to a request to know that is counted towards the limitation of two requests within a 12-month period as set forth in Civil Code section 1798.130, subdivision (b). With regard to a correction to a consumer's Social Security number, driver's license number or other government-issued identification number, financial account number, any health insurance or medical identification number, an account password, security questions and answers, or unique biometric data generated from measurements or technical analysis of human characteristics, a business shall not disclose this information, but may provide a way to confirm that the personal information it maintains is the same as what the consumer has provided.

Observations/Findings: Upon request, Thoropass will disclose specific pieces of personal information it maintains and has collected about a consumer to allow the consumer to confirm Thoropass has corrected the inaccurate information subject to a request to correct. This disclosure is not considered a response to a request to know counted towards the limitation of two (2) requests within a twelve (12) month period. Thoropass will not disclose sensitive personal information such as corrections to the following: Social Security number, driver's license number (or other government-issued identification number), financial account number, any health insurance (or medical identification number), an account password, security questions and answers, or unique biometric data generated from measurements/technical analysis of human characteristics. Thoropass will provide another way to confirm the personal information maintained is the same as what the consumer has provided. *Note: Thoropass has not received any CCPA related requests from any consumers over the last twelve (12) months.*

Recommendations: No further recommendations at this time.

K Fully Compliant

Evidence: PT-02 Authority to Process PII

Regulation:

(k) Whether a business, service provider, or contractor has implemented measures to ensure that personal information that is the subject of a request to correct remains corrected factors into whether that business, service provider, or contractor has complied with a consumer's request to correct in accordance with the CCPA and these regulations.

Observations/Findings: Thoropass, service provider, or contractor will implement measures to ensure personal information subject to a request to correct remains corrected in order to comply with a consumer's request to correct according to the CCPA and other regulations. *Note: Thoropass has not received any CCPA related requests from any consumers over the last twelve (12) months.*

Recommendations: No further recommendations at this time.

7024 Requests to Know

A Fully Compliant

Evidence: PT-02 Authority to Process PII

Regulation:

(a) For requests that seek the disclosure of specific pieces of information about the consumer, if a business cannot verify the identity of the person making the request pursuant to the regulations set forth in Article 5, the business shall not disclose any specific pieces of personal information to the requestor and shall inform the requestor that it cannot verify their identity. If the request is denied in whole or in part, the business shall also evaluate the consumer's request as if it is seeking the disclosure of categories of personal information about the consumer pursuant to subsection (b).

Observations/Findings: For disclosure of specific pieces of information, if Thoropass cannot verify the identity, Thoropass will not disclose any specific pieces of information. If the request is denied, Thoropass will evaluate the request based on seeking a disclosure of categories of personal information. If Thoropass still cannot verify the identity based on this lower threshold, Thoropass will deny the request to disclose and notify the requestor that their identity cannot be verified. Thoropass will direct the consumer to its general business practices regarding the collection, maintenance, and sale of personal information set forth in its privacy policy. *Note: Thoropass has not received any CCPA related requests from any consumers over the last twelve (12) months.*

Recommendations: No further recommendations at this time.

B Fully Compliant

Evidence: PT-02 Authority to Process PII

Regulation:

(b) For requests that seek the disclosure of categories of personal information about the consumer, if a business cannot verify the identity of the person making the request pursuant to the regulations set forth in Article 5, the business may deny the request to disclose the categories and other information requested and shall inform the requestor that it cannot verify their identity. If the request is denied in whole or in part, the business shall provide or direct the consumer to its information practices set forth in its privacy policy.

Observations/Findings: For disclosure of specific pieces of information, if Thoropass cannot verify the identity, Thoropass will not disclose any specific pieces of information. If the request is denied, Thoropass will evaluate the request based on seeking a disclosure of categories of personal information. If Thoropass still cannot verify the identity based on this lower threshold, Thoropass will deny the request to disclose and notify the requestor that their identity cannot be verified. Thoropass will direct the consumer to its general business practices regarding the collection, maintenance, and

sale of personal information set forth in its privacy policy. *Note: Thoropass has not received any CCPA related requests from any consumers over the last twelve (12) months.*

Recommendations: No further recommendations at this time.

C Fully Compliant

Evidence: PT-02 Authority to Process PII

Regulation:

(c) In responding to a request to know, a business is not required to search for personal information if all of the following conditions are met:

- (1) The business does not maintain the personal information in a searchable or reasonably accessible format;
- (2) The business maintains the personal information solely for legal or compliance purposes;
- (3) The business does not sell the personal information and does not use it for any commercial purpose.
- (4) The business describes to the consumer the categories of records that may contain personal information that it did not search because it meets the conditions stated above.

Observations/Findings: Thoropass is not required to search for personal information if all of the following conditions are met:

- Thoropass does not maintain the personal information in a searchable or reasonably accessible format;
- Thoropass maintains personal information solely for legal or compliance purposes;
- Thoropass does not sell personal information and does not use it for any commercial purposes; and
- Thoropass describes to the consumer the categories of records that may contain personal information that it did not search because it meets the conditions above.

Recommendations: No further recommendations at this time.

D Fully Compliant

Evidence: PT-02 Authority to Process PII

Regulation:

(d) A business shall not disclose in response to a request to know a consumer's Social Security number, driver's license number or other government-issued identification number, financial account number, any health insurance or medical identification number, an account password, security questions and answers, or unique biometric data generated from measurements or technical analysis of human characteristics. The business shall, however, inform the consumer with sufficient particularity that it has collected the type of information.

Observations/Findings: Thoropass will not disclose a consumer's Social Security Number, driver's license number or other government-issued identification number, financial account number, any health insurance or medical identification number, an account password, security questions and answers, or unique biometric data generated from measurements or technical analysis of human characteristics. Thoropass will inform the consumer that it collects unique biometric data including a fingerprint scan, for example, but won't disclose the actual scan. Thoropass will use reasonable security measures (like encryption) when transmitting personal information to a consumer. *Note: Thoropass has not received any CCPA related requests from any consumers over the last twelve (12) months.*

Recommendations: No further recommendations at this time.

E Fully Compliant	Evidence: PT-02 Authority to Process PII
Regulation: (e) If a business denies a consumer's verified request to know specific pieces of personal information, in whole or in part, because of a conflict with federal or state law, or an exception to the CCPA, the business shall inform the requestor and explain the basis for the denial, unless prohibited from doing so by law. If the request is denied only in part, the business shall disclose the other information sought by the consumer.	
Observations/Findings: If Thoropass denies a verified request due to a conflict or exception of law, Thoropass will inform the requester and explain the basis of the denial, unless prohibited from doing so by law. Thoropass will disclose information permitted and allowable by law to the consumer. <i>Note: Thoropass has not received any CCPA related requests from any consumers over the last twelve (12) months.</i>	
Recommendations: No further recommendations at this time.	

F Fully Compliant	Evidence: PT-02 Authority to Process PII
Regulation: (f) A business shall use reasonable security measures when transmitting personal information to the consumer.	
Observations/Findings: Thoropass will use reasonable security measures when transmitting personal information to the consumer. <i>Note: Thoropass has not received any CCPA related requests from any consumers over the last twelve (12) months.</i>	
Recommendations: No further recommendations at this time.	

G Fully Compliant	Evidence: PT-02 Authority to Process PII
Regulation: (g) If a business maintains a password-protected account with the consumer, it may comply with a request to know by using a secure self-service portal for consumers to access, view, and receive a portable copy of their personal information if the portal fully discloses the personal information that the consumer is entitled to under the CCPA and these regulations, uses reasonable data security controls, and complies with the verification requirements set forth in Article 5.	
Observations/Findings: If Thoropass maintains a password-protected account with the consumer, Thoropass will verify the consumer's identity through Thoropass's existing authentication practices for the consumer's account, provided that Thoropass follows the requirements in the CCPA regulations and uses reasonable data security controls. Thoropass will also require a consumer to re-authenticate themselves before disclosing or deleting the consumer's data.	
Recommendations: No further recommendations at this time.	

H Fully Compliant	Evidence: PT-02 Authority to Process PII
Regulation: (h) In response to a request to know, a business shall provide all the personal information it has	

collected and maintains about the consumer during the 12-month period preceding the business's receipt of the consumer's request. A consumer may request that the business provide personal information that the business collected beyond the 12-month period, as long as it was collected on or after January 1, 2022, and the business shall be required to provide that information unless doing so proves impossible or would involve disproportionate effort. That information shall include any personal information that the business's service providers or contractors collected pursuant to their written contract with the business. If a business claims that providing personal information beyond the 12-month period preceding the business's receipt of the consumer's request would be impossible or would involve disproportionate effort, the business shall not be required to provide it as long as the business provides the consumer a detailed explanation that includes enough facts to give a consumer a meaningful understanding as to why the business cannot provide personal information beyond the 12-month period. The business shall not simply state that it is impossible or would require disproportionate effort.

Observations/Findings: The disclosure of the required information shall cover the twelve (12)-month period preceding Thoropass's receipt of the verifiable individual request provided an individual may request Thoropass disclose the required information beyond the twelve (12)-month period, and Thoropass shall be required to provide information unless doing so proves impossible or would involve a disproportionate effort. An individual's right to request required information beyond the twelve(12)-month period, and Thoropass's obligation to provide the information, shall only apply to personal information collected on or after January 1, 2022. Nothing in the regulations shall require Thoropass to keep personal information for any length of time.

Thoropass receiving a verifiable individual request shall disclose any personal information it has collected about an individual, directly or indirectly, including through or by a service provider or contractor, to the individual.

A list of the categories of personal information it has collected about individuals in the preceding twelve (12) months by reference to the enumerated category or categories that most closely describe the personal information collected. The categories of sources from which an individual's personal information is collected. The business or commercial purpose for collecting, selling, or sharing consumers' personal information. The categories of third parties to whom the business discloses consumers' personal information.

Note: Thoropass has not received any CCPA related requests from any consumers over the last twelve (12) months.

Recommendations: No further recommendations at this time.

I Fully Compliant

Evidence: PT-02 Authority to Process PII

Regulation:

(i) A service provider or contractor shall provide assistance to the business in responding to a verifiable consumer request to know, including by providing the business the consumer's personal information it has in its possession that it collected pursuant to their written contract with the business, or by enabling the business to access that personal information.

Observations/Findings: A service provider (or contractor) that collects personal information pursuant to a written contract with Thoropass shall be required to assist Thoropass through appropriate technical and organizational measures in complying with the requirements of the regulation taking into account the nature of the processing.

Recommendations: No further recommendations at this time.

J Fully Compliant

Evidence: PT-02 Authority to Process PII

Regulation:

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

Observations/Findings: Thoropass will respond to a consumer's verified request to know categories of personal information with an individualized response unless Thoropass's general practices outlined in the privacy notice would be the same information required by the request to know such categories. *Note: Thoropass has not received any CCPA related requests from any consumers over the last twelve (12) months.*

Recommendations: No further recommendations at this time.

K Fully Compliant

Evidence: PT-02 Authority to Process PII

Regulation:

In responding to a verified request to know categories of personal information, the business shall provide all of the following:

- (1) The categories of personal information the business has collected about the consumer .
- (2) The categories of sources from which the personal information was collected;
- (3) The business or commercial purpose for which it collected or sold the personal information;
- (4) The categories of third parties with whom the business shares personal information;
- (5) The categories of personal information that the business sold , and for each category identified, the categories of third parties to whom it sold that particular category of personal information.
- (6) The categories of personal information that the business disclosed for a business purpose, and for each category identified, the categories of third parties to whom it disclosed that particular category of personal information.

Observations/Findings: Thoropass receiving a verifiable individual request shall disclose any personal information it has collected about an individual, directly or indirectly, including through or by a service provider or contractor, to the individual.

A list of the categories of personal information it has collected about individuals in the preceding twelve (12) months by reference to the enumerated category or categories that most closely describe the personal information collected. The categories of sources from which an individual's personal information is collected. The business or commercial purpose for collecting, selling, or sharing consumers' personal information. The categories of third parties to whom the business discloses consumers' personal information.

Note: Thoropass has not received any CCPA related requests from any consumers over the last twelve (12) months.

Recommendations: No further recommendations at this time.

L Fully Compliant

Evidence: PT-02 Authority to Process PII

Regulation:

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

Observations/Findings: A list of the categories of personal information it has collected about individuals in the preceding twelve (12) months by reference to the enumerated category or categories that most closely describe the personal information collected. The categories of sources from which an individual's personal information is collected. The business or commercial purpose for collecting, selling, or sharing consumers' personal information. The categories of third parties to whom the business discloses consumers' personal information. The list of categories will be provided to the consumer in a meaningful and understandable manner.

Note: Thoropass has not received any CCPA related requests from any consumers over the last twelve (12) months.

Recommendations: No further recommendations at this time.

7025 Opt-out Preference Signals

A Not Applicable	Evidence: N/A
------------------	----------------------

Regulation:

(a) The purpose of an opt-out preference signal is to provide consumers with a simple and easy- to-use method by which consumers interacting with businesses online can automatically exercise their right to opt-out of sale/sharing. Through an opt-out preference signal, a consumer can opt-out of sale and sharing of their personal information with all businesses they interact with online without having to make individualized requests with each business.

Observations/Findings: NA. Thoropass does not sell or share personal information and does not require an opt-out preference signal.

Recommendations: Not applicable.

B Not Applicable	Evidence: N/A
------------------	----------------------

Regulation:

(b) A business that sells or shares personal information shall process any opt-out preference signal that meets the following requirements as a valid request to opt-out of sale/sharing:

(1) The signal shall be in a format commonly used and recognized by businesses. An example would be an HTTP header field or JavaScript object.

(2) The platform, technology, or mechanism that sends the opt-out preference signal shall make clear to the consumer, whether in its configuration or in disclosures to the public, that the use of the signal is meant to have the effect of opting the consumer out of the sale and sharing of their personal information. The configuration or disclosure does not need to be tailored only to California or to refer to California.

Observations/Findings: NA. Thoropass does not sell or share personal information and does not require an opt-out preference signal.

Recommendations: Not applicable.

C Not Applicable

Evidence: N/A

Regulation:

(c) When a business that collects personal information from consumers online receives or detects an opt-out preference signal that complies with subsection (b):

(1) The business shall treat the opt-out preference signal as a valid request to opt-out of sale/sharing submitted pursuant to Civil Code section 1798.120 for that browser or device and any consumer profile associated with that browser or device, including pseudonymous profiles. If known, the business shall also treat the opt-out preference signal as a valid request to opt-out of sale/sharing for the consumer. This is not required for a business that does not sell or share personal information.

(2) The business shall not require a consumer to provide additional information beyond what is necessary to send the signal. However, a business may provide the consumer with an option to provide additional information if it will help facilitate the consumer's request to opt-out of sale/sharing. Any information provided by the consumer shall not be used, disclosed, or retained for any purpose other than processing the request to opt-out of sale/sharing.

(3) If the opt-out preference signal conflicts with a consumer's business-specific privacy setting that allows the business to sell or share their personal information, the business shall process the opt-out preference signal as a valid request to opt-out of sale/sharing, but may notify the consumer of the conflict and provide the consumer with an opportunity to consent to the sale or sharing of their personal information. The business shall comply with section 7004 in obtaining the consumer's consent to the sale or sharing of their personal information. If the consumer consents to the sale or sharing of their personal information, the business may ignore the opt-out preference signal for as long as the consumer is known to the business.

(4) If the opt-out preference signal conflicts with the consumer's participation in a business's financial incentive program that requires the consumer to consent to the sale or sharing of personal information, the business may notify the consumer that processing the opt-out preference signal as a valid request to opt-out of sale/sharing would withdraw the consumer from the financial incentive program and ask the consumer to affirm that they intend to withdraw from the financial incentive program. If the consumer affirms that they intend to withdraw from the financial incentive program, the business shall process the consumer's request to opt-out of sale/sharing. If the business asks and the consumer does not affirm their intent to withdraw, the business may ignore the opt-out preference signal with respect to that consumer's participation in the financial incentive program for as long as the consumer is known to the business. If the business does not ask the consumer to affirm their intent with regard to the financial incentive program, the business shall still process the opt-out preference signal as a valid request to opt-out of sale/sharing for that browser or device and any consumer profile the business associates with that browser or device.

(5) Where the consumer is known to the business, the business shall not interpret the absence of an opt-out preference signal after the consumer previously sent an opt-out preference signal as consent to opt-in to the sale or sharing of personal information.

(6) A business may display whether it has processed the consumer's opt-out preference signal as a valid request to opt-out of sale/sharing on its website.

Observations/Findings: NA. Thoropass does not sell or share personal information and does not require an opt-out preference signal.

Recommendations: Not applicable.

D Not Applicable	Evidence: N/A
<p>Regulation: (d) The business and the platform, technology, or mechanism that sends the opt-out preference signal shall not use, disclose, or retain any personal information collected from the consumer in connection with the sending or processing the request to opt-out of sale/sharing for any purpose other than sending or processing the opt-out preference signal.</p>	
<p>Observations/Findings: NA. Thoropass does not sell or share personal information and does not require an opt-out preference signal.</p>	
<p>Recommendations: Not applicable.</p>	

E Not Applicable	Evidence: N/A
<p>Regulation: (e) Civil Code section 1798.135, subdivisions (b)(1) and (3), provide a business the choice between (1) processing opt-out preference signals and providing the “Do Not Sell or Share My Personal Information” and “Limit the Use of My Sensitive Personal Information” links or the Alternative Opt-out Link; or (2) processing opt-out preference signals in a frictionless manner in accordance with these regulations and not having to provide the “Do Not Sell or Share My Personal Information” and “Limit the Use of My Sensitive Personal Information” links or the Alternative Opt-out Link. They do not give the business the choice between posting the above-referenced links or honoring opt-out preference signals. Even if the business posts the above-referenced links, the business must still process opt-out preference signals, though it may do so in a non-frictionless manner. If a business processes opt-out preference signals in a frictionless manner in accordance with subsections (f) and (g), then it may, but is not required to, provide the above-referenced links.</p>	
<p>Observations/Findings: NA. Thoropass does not sell or share personal information and does not require an opt-out preference signal.</p>	
<p>Recommendations: Not applicable.</p>	

F Not Applicable	Evidence: N/A
<p>Regulation: (f) Except as allowed by these regulations, processing an opt-out preference signal in a frictionless manner as required by Civil Code section 1798.135, subdivision (b)(1), means that the business shall not: (1) Charge a fee or require any valuable consideration if the consumer uses an opt-out preference signal. (2) Change the consumer’s experience with the product or service offered by the business. (3) Display a notification, pop-up, text, graphic, animation, sound, video, or any interstitial content in response to the opt-out preference signal. However, a business’s display of whether the consumer visiting their website has opted out of the sale or sharing their personal information shall not be considered a violation of this regulation. The business may also provide a link to a privacy settings page, menu, or similar interface that enables the consumer to consent to the business ignoring the opt-out preference signal with respect to the business’s sale or sharing of the consumer’s personal information provided that it complies with subsections (f)(1) through (3).</p>	
<p>Observations/Findings: NA. Thoropass does not sell or share personal information and does not require an opt-out preference signal.</p>	

Recommendations: Not applicable.

G Not Applicable

Evidence: N/A

Regulation:

(g) A business meeting the requirements of Civil Code section 1798.135, subdivision (b)(1) is not required to post the “Do Not Sell or Share My Personal Information” link or the Alternative Opt-out Link if it meets all of the following additional requirements:

(1) Processes the opt-out preference signal in a frictionless manner in accordance with the CCPA and these regulations.

(2) Includes in its privacy policy the following information:

(A) A description of the consumer’s right to opt-out of the sale or sharing of their personal information by the business;

(B) A statement that the business processes opt-out preference signals in a frictionless manner;

(C) Information on how consumers can implement opt-out preference signals for the business to process in frictionless manner; and

(D) Instructions for any other method by which the consumer may submit a request to opt-out of sale/sharing.

(3) Allows the opt-out preference signal to fully effectuate the consumer’s request to opt- out of sale/sharing.

Observations/Findings: NA. Thoropass does not sell or share personal information and does not require an opt-out preference signal.

Recommendations: Not applicable.

7026 Requests to Opt-out of Sale/Sharing

A Not Applicable

Evidence: N/A

Regulation:

(a) A business that sells or shares personal information shall provide two or more designated methods for submitting requests to opt-out of sale/sharing. A business shall consider the methods by which it interacts with consumers, the manner in which the business collects the personal information that it makes available to third parties, available technology, and ease of use by the consumer when determining which methods consumers may use to submit requests to opt-out of sale/sharing. At least one method offered shall reflect the manner in which the business primarily interacts with the consumer. Illustrative examples follow.

(1) A business that collects personal information from consumers online shall, at a minimum, allow consumers to submit requests to opt-out of sale/sharing through an opt-out preference signal and at least one of the following methods: an interactive form accessible via the “Do Not Sell or Share My Personal Information” link, the Alternative Opt-out Link, or the business’s privacy policy if the business processes an opt-out preference signal in a frictionless manner.

(2) A business that interacts with consumers in person and online may provide an in- person method for submitting requests to opt-out of sale/sharing in addition to the opt-out preference signal.

(3) Other methods for submitting requests to opt-out of the sale/sharing include, but are not limited to, a toll-free phone number, a designated email address, a form submitted in person, and a form submitted through the mail.

(4) A notification or tool regarding cookies, such as a cookie banner or cookie controls, is not by itself an acceptable method for submitting requests to opt-out of sale/sharing because cookies concern the collection of personal information and not the sale or sharing of personal information. An acceptable method for submitting requests to opt- out of sale/sharing must address the sale and sharing of personal information.

Observations/Findings: N/A. Thoropass does not sell or share personal information and does not require a method to opt-out of sale/sharing.

Recommendations: Not applicable.

B Not Applicable

Evidence: N/A

Regulation:

(b) A business's methods for submitting requests to opt-out of sale/sharing shall be easy for consumers to execute, shall require minimal steps, and shall comply with section 7004

Observations/Findings: N/A. Thoropass does not sell or share personal information and does not require a method to opt-out of sale/sharing.

Recommendations: Not applicable.

C Not Applicable

Evidence: N/A

Regulation:

(c) A business shall not require a consumer submitting a request to opt-out of sale/sharing to create an account or provide additional information beyond what is necessary to direct the business not to sell or share the consumer's personal information.

Observations/Findings: N/A. Thoropass does not sell or share personal information and does not require a method to opt-out of sale/sharing.

Recommendations: Not applicable.

D Not Applicable

Evidence: N/A

Regulation:

(d) A business shall not require a verifiable consumer request for a request to opt-out of sale/sharing. A business may ask the consumer for information necessary to complete the request, such as information necessary to identify the consumer whose information shall cease to be sold or shared by the business. However, to the extent that the business can comply with a request to opt-out of sale/sharing without additional information, it shall do so.

Observations/Findings: N/A. Thoropass does not sell or share personal information and does not require a method to opt-out of sale/sharing.

Recommendations: Not applicable.

E Not Applicable

Evidence: N/A

Regulation:

(e) If a business has a good-faith, reasonable, and documented belief that a request to opt-out of sale/sharing is fraudulent, the business may deny the request. The business shall inform the requestor that it will not comply with the request and shall provide to the requestor an explanation why it believes the request is fraudulent.

Observations/Findings: N/A. Thoropass does not sell or share personal information and does not require a method to opt-out of sale/sharing.

Recommendations: Not applicable.

F Not Applicable

Evidence: N/A

Regulation:

(f) A business shall comply with a request to opt-out of sale/sharing by:
 (1) Ceasing to sell to and/or share with third parties the consumer’s personal information as soon as feasibly possible, but no later than 15 business days from the date the business receives the request. Service providers or contractors collecting personal information pursuant to the written contract with the business required by the CCPA and these regulations does not constitute a sale or sharing of personal information.
 (2) Notifying all third parties to whom the business has sold or shared the consumer’s personal information, after the consumer submits the request to opt-out of sale/sharing and before the business complies with that request, that the consumer has made a request to opt-out of sale/sharing and directing them to comply with the consumer’s request and forward the request to any other person to whom the third party has made the personal information available during that time period.

Observations/Findings: N/A. Thoropass does not sell or share personal information and does not require a method to opt-out of sale/sharing.

Recommendations: Not applicable.

G Not Applicable

Evidence: N/A

Regulation:

(g) A business may provide a means by which the consumer can confirm that their request to opt-out of sale/sharing has been processed by the business. For example, the business may display on its website “Consumer Opted Out of Sale/Sharing” or display through a toggle or radio button that the consumer has opted out of the sale/sharing of their personal information.

Observations/Findings: N/A. Thoropass does not sell or share personal information and does not require a method to opt-out of sale/sharing.

Recommendations: Not applicable.

H Not Applicable

Evidence: N/A

Regulation:

(h) In responding to a request to opt-out of sale/sharing, a business may present the consumer with the choice to opt-out of the sale or sharing of personal information for certain uses as long as a single option to opt-out of the sale or sharing of all personal information is also offered . However, doing so in

response to an opt-out preference signal will prevent the business from using the exception set forth in Civil Code section 1798.135, subdivision (b)(1).

Observations/Findings: N/A. Thoropass does not sell or share personal information and does not require a method to opt-out of sale/sharing.

Recommendations: Not applicable.

I Not Applicable

Evidence: N/A

Regulation:

(i) A business that responds to a request to opt-out of sale/sharing by informing the consumer of a charge for the use of any product or service shall comply with Article 7 and shall provide the consumer with a Notice of Financial Incentive that complies with section 7016 in its response. However, doing so in response to an opt-out preference signal will prevent the business from using the exception set forth in Civil Code section 1798.135, subdivision (b)(1).

Observations/Findings: N/A. Thoropass does not sell or share personal information and does not require a method to opt-out of sale/sharing.

Recommendations: Not applicable.

J Not Applicable

Evidence: N/A

Regulation:

(j) A consumer may use an authorized agent to submit a request to opt-out of sale/sharing on the consumer's behalf if the consumer provides the authorized agent written permission signed by the consumer. A business may deny a request from an authorized agent if the agent does not provide to the business the consumer's signed permission demonstrating that they have been authorized by the consumer to act on the consumer's behalf. The requirement to obtain and provide written permission from the consumer does not apply to requests made by an opt-out preference signal.

Observations/Findings: N/A. Thoropass does not sell or share personal information and does not require a method to opt-out of sale/sharing.

Recommendations: Not applicable.

K Not Applicable

Evidence: N/A

Regulation:

(k) Except as allowed by these regulations, a business shall wait at least 12 months from the date of the consumer's request before asking a consumer who has opted out of the sale or sharing of their personal information to consent to the sale or sharing of their personal information.

Observations/Findings: N/A. Thoropass does not sell or share personal information and does not require a method to opt-out of sale/sharing.

Recommendations: Not applicable.

7027 Requests to Limit Use and Disclosure of Sensitive Personal Information

A Not Applicable	Evidence: N/A
<p>Regulation: (a) The unauthorized use or disclosure of sensitive personal information creates a heightened risk of harm for the consumer. The purpose of the request to limit is to give consumers meaningful control over how their sensitive personal information is collected, used, and disclosed. It gives the consumer the ability to limit the business’s use of sensitive personal information to that which is necessary to perform the services or provide the goods reasonably expected by an average consumer who requests those goods or services, with some narrowly tailored exceptions, which are set forth in subsection (m). Sensitive personal information that is collected or processed without the purpose of inferring characteristics about a consumer is not subject to requests to limit.</p>	
<p>Observations/Findings: N/A. Thoropass only uses or discloses sensitive personal information under reasonably necessary use/disclosure and proportionate purposes, which exempts Thoropass from the requirement to post a Notice of Right to Limit.</p>	
<p>Recommendations: Not applicable.</p>	

B Not Applicable	Evidence: N/A
<p>Regulation: (b) A business that uses or discloses sensitive personal information for purposes other than those set forth in subsection (m) shall provide two or more designated methods for submitting requests to limit. A business shall consider the methods by which it interacts with consumers, the manner in which the business collects the sensitive personal information that it uses for purposes other than those set forth in subsection (m), available technology, and ease of use by the consumer when determining which methods consumers may use to submit requests to limit. At least one method offered shall reflect the manner in which the business primarily interacts with the consumer. Illustrative examples follow. (1) A business that collects sensitive personal information from consumers online shall, at a minimum, allow consumers to submit requests to limit through an interactive form accessible via the “Limit the Use of My Sensitive Personal Information” link or the Alternative Opt-out Link. (2) A business that interacts with consumers in person and online may provide an in- person method for submitting requests to limit in addition to the online form. (3) Other methods for submitting requests to limit include, but are not limited to, a toll- free phone number, a designated email address, a form submitted in person, and a form submitted through the mail. (4) A notification or tool regarding cookies, such as a cookie banner or cookie controls, is not by itself an acceptable method for submitting requests to limit because cookies concern the collection of personal information and not necessarily the use and disclosure of sensitive personal information. An acceptable method for submitting requests to limit must address the specific right to limit.</p>	
<p>Observations/Findings: N/A. Thoropass only uses or discloses sensitive personal information under reasonably necessary use/disclosure and proportionate purposes, which exempts Thoropass from the requirement of having two (2) or more designated methods for submitting requests to limit.</p>	
<p>Recommendations: Not applicable.</p>	

C Not Applicable	Evidence: N/A
------------------	----------------------

Regulation:

(c) A business's methods for submitting requests to limit shall be easy for consumers to execute, shall require minimal steps, and shall comply with section 7004.

Observations/Findings: N/A. Thoropass only uses or discloses sensitive personal information under reasonably necessary use/disclosure and proportionate purposes, which exempts Thoropass from the requirement of having two (2) or more designated methods for submitting requests to limit.

Recommendations: Not applicable.

D Not Applicable

Evidence: N/A

Regulation:

(d) A business shall not require a consumer submitting a request to limit to create an account or provide additional information beyond what is necessary to direct the business to limit the use or disclosure of the consumer's sensitive personal information.

Observations/Findings: N/A. Thoropass only uses or discloses sensitive personal information under reasonably necessary use/disclosure and proportionate purposes, which exempts Thoropass from the requirement to post a Notice of Right to Limit.

Recommendations: Not applicable.

E Not Applicable

Evidence: N/A

Regulation:

(e) A business shall not require a verifiable consumer request for a request to limit. A business may ask the consumer for information necessary to complete the request, such as information necessary to identify the consumer to whom the request should be applied. However, to the extent that the business can comply with a request to limit without additional information, it shall do so.

Observations/Findings: N/A. Thoropass only uses or discloses sensitive personal information under reasonably necessary use/disclosure and proportionate purposes, which exempts Thoropass from the requirement to post a Notice of Right to Limit.

Recommendations: Not applicable.

F Not Applicable

Evidence: N/A

Regulation:

(f) If a business has a good-faith, reasonable, and documented belief that a request to limit is fraudulent, the business may deny the request. The business shall inform the requestor that it will not comply with the request and shall provide to the requestor an explanation why it believes the request is fraudulent.

Observations/Findings: N/A. Thoropass only uses or discloses sensitive personal information under reasonably necessary use/disclosure and proportionate purposes, which exempts Thoropass from the requirement to post a Notice of Right to Limit.

Recommendations: Not applicable.

G Not Applicable	Evidence: N/A
<p>Regulation: (g) A business shall comply with a request to limit by: (1) Ceasing to use and disclose the consumer’s sensitive personal information for purposes other than those set forth in subsection (m) as soon as feasibly possible, but no later than 15 business days from the date the business receives the request. (2) Notifying all the business’s service providers or contractors that use or disclose the consumer’s sensitive personal information for purposes other than those set forth in subsection (m) that the consumer has made a request to limit and instructing them to comply with the consumer’s request to limit within the same time frame. (3) Notifying all third parties to whom the business has disclosed or made available the consumer’s sensitive personal information for purposes other than those set forth in subsection (m), after the consumer submitted their request and before the business complies with that request, that the consumer has made a request to limit and direct them 1) to comply with the consumer’s request and 2) to forward the request to any other person with whom the third party has disclosed or shared the sensitive personal information during that time period.</p>	
<p>Observations/Findings: N/A. Thoropass only uses or discloses sensitive personal information under reasonably necessary use/disclosure and proportionate purposes, which exempts Thoropass from the requirement to post a Notice of Right to Limit.</p>	
<p>Recommendations: Not applicable.</p>	

H Not Applicable	Evidence: N/A
<p>Regulation: (h) A business may provide a means by which the consumer can confirm that their request to limit has been processed by the business. For example, the business may display through a toggle or radio button that the consumer has limited the business’s use and disclosure of their sensitive personal information.</p>	
<p>Observations/Findings: N/A. Thoropass only uses or discloses sensitive personal information under reasonably necessary use/disclosure and proportionate purposes, which exempts Thoropass from the requirement to post a Notice of Right to Limit.</p>	
<p>Recommendations: Not applicable.</p>	

I Not Applicable	Evidence: N/A
<p>Regulation: (i) In responding to a request to limit, a business may present the consumer with the choice to allow specific uses for the sensitive personal information as long as a single option to limit the use of the personal information is also offered.</p>	
<p>Observations/Findings: N/A. Thoropass only uses or discloses sensitive personal information under reasonably necessary use/disclosure and proportionate purposes, which exempts Thoropass from the requirement to post a Notice of Right to Limit.</p>	
<p>Recommendations: Not applicable.</p>	

J Not Applicable	Evidence: N/A
<p>Regulation: (j) A consumer may use an authorized agent to submit a request to limit on the consumer’s behalf if the consumer provides the authorized agent written permission signed by the consumer. A business may deny a request from an authorized agent if the agent does not provide to the business the consumer’s signed permission demonstrating that they have been authorized by the consumer to act on the consumer’s behalf.</p>	
<p>Observations/Findings: N/A. Thoropass only uses or discloses sensitive personal information under reasonably necessary use/disclosure and proportionate purposes, which exempts Thoropass from the requirement to post a Notice of Right to Limit.</p>	
<p>Recommendations: Not applicable.</p>	

K Not Applicable	Evidence: N/A
<p>Regulation: (k) A business that responds to a request to limit by informing the consumer of a charge for the use of any product or service shall comply with Article 7 and shall provide the consumer with a Notice of Financial Incentive that complies with section 7016 in its response.</p>	
<p>Observations/Findings: N/A. Thoropass only uses or discloses sensitive personal information under reasonably necessary use/disclosure and proportionate purposes, which exempts Thoropass from the requirement to post a Notice of Right to Limit.</p>	
<p>Recommendations: Not applicable.</p>	

L Not Applicable	Evidence: N/A
<p>Regulation: (l) Except as allowed by these regulations, a business shall wait at least 12 months from the date the consumer’s request to limit is received before asking a consumer who has exercised their right to limit to consent to the use or disclosure of their sensitive personal information for purposes other than those set forth in subsection (m).</p>	
<p>Observations/Findings: N/A. Thoropass only uses or discloses sensitive personal information under reasonably necessary use/disclosure and proportionate purposes, which exempts Thoropass from the requirement to post a Notice of Right to Limit.</p>	
<p>Recommendations: Not applicable.</p>	

M Not Applicable	Evidence: N/A
<p>Regulation: (m) The purposes identified in Civil Code section 1798.121, subdivision (a), for which a business may use or disclose sensitive personal information without being required to offer consumers a right to limit are as follows. A business that only uses or discloses sensitive personal information for these purposes, provided that the use or disclosure is reasonably necessary and proportionate for those</p>	

purposes, is not required to post a Notice of Right to Limit or provide a method for submitting a request to limit.

- (1) To perform the services or provide the goods reasonably expected by an average consumer who requests those goods or services.
- (2) To prevent, detect, and investigate security incidents that compromise the availability, authenticity, integrity, or confidentiality of stored or transmitted personal information.
- (3) To resist malicious, deceptive, fraudulent, or illegal actions directed at the business and to prosecute those responsible for those actions.
- (4) To ensure the physical safety of natural persons.
- (5) For short-term, transient use, including, but not limited to, nonpersonalized advertising shown as part of a consumer's current interaction with the business, provided that the 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 the business.
- (6) To perform services on behalf of the business.
- (7) To verify or maintain the quality or safety of a product, service, or device that is owned, manufactured, manufactured for, or controlled by the business, and to improve, upgrade, or enhance the service or device that is owned, manufactured by, manufactured for, or controlled by the business.
- (8) To collect or process sensitive personal information where the collection or processing is not for the purpose of inferring characteristics about a consumer.

Observations/Findings: N/A. Thoropass only uses or discloses sensitive personal information for the following purposes under reasonably necessary use/disclosure and proportionate purposes, which exempts Thoropass from the requirement to post a Notice of Right to Limit:

- To perform Thoropass's services or provide the Thoropass's product reasonably expected by an average consumer who requests these goods or services.
- To prevent, detect, and investigate security incidents compromising the availability, authenticity, integrity, or confidentiality of stored/transmitted personal information.
- To resist malicious, deceptive, fraudulent, or illegal actions directed at Thoropass and to prosecute those responsible for those actions.
- To ensure the physical safety of natural persons.
- For short-term, transient use, include, but not limited to, non-personalized advertising shown as part of a consumer's current interaction with Thoropass, provided: Thoropass does not disclose personal information to another third party; does not use this personal information to build a profile about the consumer; or otherwise alter the consumer's experience outside the current interaction with Thoropass.
- To perform services on behalf of Thoropass.
- To verify or maintain the quality or safety of Thoropass's products or services and to improve, upgrade, or enhance the product or service.
- To collect or process sensitive personal information where the collection/processing is not for the purpose of inferring characteristics about a consumer.

Recommendations: Not applicable.

7028 Requests to Opt-in After Opting-out of the Sale or Sharing of Personal Information

A Not Applicable

Evidence: N/A

Regulation:

(a) Requests to opt-in to sale or sharing of personal information shall use a two-step opt-in process whereby the consumer shall first, clearly request to opt-in and then second, separately confirm their choice to opt-in.

Observations/Findings: N/A. Thoropass does not sell or share personal information and does not provide for the right to opt-in after opting-out of the sale/share of personal information.

Recommendations: Not applicable.

B Not Applicable

Evidence: N/A

Regulation:

(b) If a consumer who has opted-out of the sale or sharing of their personal information initiates a transaction or attempts to use a product or service that requires the sale or sharing of their personal information, the business may inform the consumer that the transaction, product, or service requires the sale or sharing of their personal information and provide instructions on how the consumer can provide consent to opt-in to the sale or sharing of their personal information. The business shall comply with section 7004 when obtaining the consumer’s consent.

Observations/Findings: N/A. Thoropass does not sell or share personal information and does not provide for the right to opt-in after opting-out of the sale/share of personal information.

Recommendations: Not applicable.

Article 4 Service Providers, Contractors, and Third Parties

7050 Service Providers and Contractors

A Fully Compliant

Evidence: PT-03 PII Processing Purposes; SR - Third Party Risk Management Policy and Procedures

Regulation:

(a) A service provider or contractor shall not retain, use, or disclose personal information collected pursuant to its written contract with the business except:

- (1) For the specific business purpose(s) set forth in the written contract between the business and the service provider or contractor that is required by the CCPA and these regulations.;
- (2) To retain and employ another service provider or contractor as a subcontractor, where the subcontractor meets the requirements for a service provider or contractor under the CCPA and these regulations.
- (3) For internal use by the service provider or contractor to build or improve the quality of the services it is providing to the business, even if this business purpose is not specified in the written contract required by the CCPA and these regulations, provided that the service provider or contractor does not use the personal information to perform services on behalf of another person.
- (4) To prevent, detect, or investigate data security incidents or protect against malicious, deceptive, fraudulent or illegal activity, even if this business purpose is not specified in the written contract required by the CCPA and these regulations.
- (5) For the purposes enumerated in Civil Code section 1798.145, subdivisions (a)(1) through (a)(7).

Observations/Findings: Service providers or contractors of Thoropass will not retain, use, or disclose personal information collected pursuant to written contracts with Thoropass except for the following:

- Specific business purposes within written contracts between Thoropass and the service provider/contractor required by the CCPA;
- To retain/employ another service provider/contractor as a subcontractor meeting the same

requirements as those between the service provider/contractor and Thoropass as well as the CCPA regulations;

- For internal use by service provider/contractor to build/improve the quality of services provided to Thoropass even if the business purpose is not specified in written contract required by the CCPA provided the service provider/contractor does not use personal information to perform services on behalf of another person;
- To prevent, detect, or investigate data security incidents or protect against malicious, deceptive, fraudulent, or illegal activities even if this purpose is not specified in written contract required by the CCPA;
- To comply with federal, state, or local laws or comply with a court order or subpoena to provide information.
- To comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, or local authorities. Law enforcement agencies, including police and sheriff's departments, may direct a business pursuant to a law enforcement agency-approved investigation with an active case number not to delete a consumer's personal information, and, upon receipt of that direction, a business shall not delete the personal information for 90 days in order to allow the law enforcement agency to obtain a court-issued subpoena, order, or warrant to obtain a consumer's personal information. For good cause and only to the extent necessary for investigatory purposes, a law enforcement agency may direct a business not to delete the consumer's personal information for additional 90-day periods. A business that has received direction from a law enforcement agency not to delete the personal information of a consumer who has requested deletion of the consumer's personal information shall not use the consumer's personal information for any purpose other than retaining it to produce to law enforcement in response to a court-issued subpoena, order, or warrant unless the consumer's deletion request is subject to an exemption from deletion under this title.
- To cooperate with law enforcement agencies concerning conduct or activity that the business, service provider, or third party reasonably and in good faith believes may violate federal, state, or local law.
- To cooperate with a government agency request for emergency access to a consumer's personal information if a natural person is at risk or danger of death or serious physical injury provided that:
 - The request is approved by a high-ranking agency officer for emergency access to a consumer's personal information.
 - The request is based on the agency's good faith determination that it has a lawful basis to access the information on a non-emergency basis.
 - The agency agrees to petition a court for an appropriate order within three days and to destroy the information if that order is not granted.
 - Exercise or defend legal claims.
- Collect, use, retain, sell, share, or disclose consumers' personal information that is deidentified or aggregate consumer information.
- Collect, sell, or share a consumer's personal information if every aspect of that commercial conduct takes place wholly outside of California. Note: For purposes of this title, commercial conduct takes place wholly outside of California if the business collected that information while the consumer was outside of California, no part of the sale of the consumer's personal information occurred in California, and no personal information collected while the consumer was in California is sold. This paragraph shall not prohibit a business from storing, including on a device, personal information about a consumer when the consumer is in California and then collecting that personal information when the consumer and stored personal information is outside of California.

Recommendations: No further recommendations at this time.

B Fully Compliant

Evidence: PT-03 PII Processing Purposes; SR - Third Party Risk Management Policy and Procedures

Regulation:

(b) A service provider or contractor cannot contract with a business to provide cross-context behavioral advertising. Pursuant to Civil Code section 1798.140, subdivision (e)(6), a service provider or contractor may contract with a business to provide advertising and marketing services, but the service provider or contractor shall not combine the personal information of consumers who have opted-out of the sale/sharing that the service provider or contractor receives from, or on behalf of, the business with personal information that the service provider or contractor receives from, or on behalf of, another person or collects from its own interaction with consumers. A person who contracts with a business to provide cross-context behavioral advertising is a third party and not a service provider or contractor with respect to cross-context behavioral advertising services.

Observations/Findings: Thoropass does not permit a service provider or contractor to contract with Thoropass to provide cross-context behavioral advertising.

Recommendations: No further recommendations at this time.

C Fully Compliant

Evidence: PT-03 PII Processing Purposes; SR - Third Party Risk Management Policy and Procedures

Regulation:

(c) If a service provider or contractor receives a request made pursuant to the CCPA directly from the consumer, the service provider or contractor shall either act on behalf of the business in accordance with the business's instructions for responding to the request or inform the consumer that the request cannot be acted upon because the request has been sent to a service provider or contractor.

Observations/Findings: If Thoropass, as a service provider, receives a request to know or a request to delete from a consumer, Thoropass will either act on behalf of the business in responding to the request or inform the consumer that the request cannot be acted upon because the request has been sent to a service provider. Thoropass, as a service provider that is a business, will comply with the CCPA regulations with regard to any personal information that it collects, maintains, or sells outside of its role as a service provider.

Recommendations: No further recommendations at this time.

D Fully Compliant

Evidence: PT-03 PII Processing Purposes; SR - Third Party Risk Management Policy and Procedures

Regulation:

(d) A service provider or contractor that is a business shall comply with the CCPA and these regulations with regard to any personal information that it collects, maintains, or sells outside of its role as a service provider or contractor.

Observations/Findings: All Thoropass's service providers or contractors will comply with the CCPA with regards to any personal information they collect, maintain, or sell outside of its role as a service provider or contractor.

Recommendations: No further recommendations at this time.

E Fully Compliant

Evidence: PT-03 PII Processing Purposes; SR - Third Party Risk Management Policy and Procedures

Regulation: (e) A person who does not have a contract that complies with section 7051, subsection (a), is not a service provider or a contractor under the CCPA.	
Observations/Findings: Thoropass maintains contracts with all service providers or contractors complying with the CCPA.	
Recommendations: No further recommendations at this time.	

F Fully Compliant	Evidence: PT-03 PII Processing Purposes; SR - Third Party Risk Management Policy and Procedures
Regulation: (f) A service provider or a contractor shall comply with the terms of the contract required by the CCPA and these regulations.	
Observations/Findings: All Thoropass's service providers or contractors will comply with the CCPA with regards to any personal information they collect, maintain, or sell outside of its role as a service provider or contractor.	
Recommendations: No further recommendations at this time.	

G Not Applicable	Evidence: N/A
Regulation: (g) Whether an entity that provides services to a nonbusiness must comply with a consumer's CCPA request depends upon whether the entity is a "business," as defined by Civil Code section 1798.140, subdivision (d).	
Observations/Findings: N/A. Thoropass is considered a business under CCPA and all service providers or contractors must comply with the CCPA.	
Recommendations: Not applicable.	

7051 Contract Requirements for Service Providers and Contractors

A Fully Compliant	Evidence: SR-Third Party Risk Management Procedures; Contract Review
Regulation: (a) The contract required by the CCPA for service providers and contractors shall: (1) Prohibit the service provider or contractor from selling or sharing personal information it collects pursuant to the written contract with the business. (2) Identify the specific business purpose(s) for which the service provider or contractor is processing personal information pursuant to the written contract with the business, and specify that the business is disclosing the personal information to the service provider or contractor only for the limited and specified business purpose(s) set forth within the contract. The business purpose(s) shall not be described in generic terms, such as referencing the entire contract generally. The description shall be specific. (3) Prohibit the service provider or contractor from retaining, using, or disclosing the personal information that it collected pursuant to the written contract with the business for any purpose other	

than the business purpose(s) specified in the contract or as otherwise permitted by the CCPA and these regulations.

(4) Prohibit the service provider or contractor from retaining, using, or disclosing the personal information that it collected pursuant to the written contract with the business for any commercial purpose other than the business purpose(s) specified in the contract, unless expressly permitted by the CCPA or these regulations.

(5) Prohibit the service provider or contractor from retaining, using, or disclosing the personal information that it collected pursuant to the written contract with the business outside the direct business relationship between the service provider or contractor and the business, unless expressly permitted by the CCPA or these regulations.

(6) Require the service provider or contractor to comply with all applicable sections of the CCPA and these regulations, including—with respect to the personal information that it collected pursuant to the written contract with the business—providing the same level of privacy protection as required of businesses by the CCPA and these regulations.

(7) Grant the business the right to take reasonable and appropriate steps to ensure that the service provider or contractor uses the personal information that it collected pursuant to the written contract with the business in a manner consistent with the business's obligations under the CCPA and these regulations. Reasonable and appropriate steps may include ongoing manual reviews and automated scans of the service provider's system and regular internal or third-party assessments, audits, or other technical and operational testing at least once every 12 months.

(8) Require the service provider or contractor to notify the business after it makes a determination that it can no longer meet its obligations under the CCPA and these regulations.

(9) Grant the business the right, upon notice, to take reasonable and appropriate steps to stop and remediate the service provider or contractor's unauthorized use of personal information.

(10) Require the service provider or contractor to enable the business to comply with consumer requests made pursuant to the CCPA or require the business to inform the service provider or contractor of any consumer request made pursuant to the CCPA that they must comply with and provide the information necessary for the service provider or contractor to comply with the request.

Observations/Findings: Thoropass performs contract reviews to ensure service providers and contractors of Thoropass meet the requirements of CCPA to include:

- Prohibit Sale/Sharing: Ensure contract prohibits the selling or sharing of personal information collected
- Limited and Specified Business Purposes: Ensure contract identifies specific business purposes for which personal information is being processed and specify information is disclosed only for the limited/specified business purpose(s). Ensure description is specific.
- Prohibit Retention, Use, Disclosure Other Than in Contract: Ensure contract prohibits retaining, using, or disclosing personal information for any purpose other than specified in contract (or otherwise permitted by the CCPA).
- Prohibit Retention, Use, Disclosure Other Commercial Purpose: Ensure contract prohibits retaining, using, or disclosing personal information for any commercial purpose other than specified in contract (unless expressly permitted by the CCPA).
- Prohibit Retention, Use, Disclosure Outside of Business Relationship: Ensure contract prohibits retaining, using, or disclosing personal information outside the direct business relationship (unless expressly permitted by the CCPA).
- Require Compliance with the CCPA and provide same level of Privacy Protection: Ensure contract requires compliance with all applicable sections of the CCPA and provide for the same level of privacy protection as required by the CCPA
- Grant Right to Review: Ensure contract provides for the right to take reasonable and appropriate steps to ensure compliance with CCPA (to include ongoing manual reviews, automated scans, internal/third-party assessments, audits, or other technical/operational testing at least once every twelve (12) months).
- Notification: Ensure contract requires notification after a determination is made service provider/contractor can no longer meet CCPA obligations/requirements.
- Right to Stop/Remediate Unauthorized Use: Ensure contract provides for the right, upon notice,

<p>to take reasonable and appropriate steps to stop and remediate any unauthorized use of personal information to include providing documentation verifying personal information is no longer retained or used once a valid request to delete was made.</p> <ul style="list-style-type: none"> • Comply with Consumer Requests: Ensure contract provides for the enablement to comply with consumer requests pursuant to CCPA (or require Thoropass to inform service provider/contractor to comply with any consumer requests made) and provide the necessary information to comply with request.
<p>Recommendations: No further recommendations at this time.</p>

<p>B Fully Compliant</p>	<p>Evidence: SR-Third Party Risk Management Procedures; Contract Review</p>
<p>Regulation: (b) A service provider or contractor that subcontracts with another person in providing services to the business for whom it is a service provider or contractor shall have a contract with the subcontractor that complies with the CCPA and these regulations, including subsection (a).</p>	
<p>Observations/Findings: Thoropass performs contract reviews to ensure contract stipulates subcontractors working with service provider/contractor must have a contract in place complying within the CCPA and items above.</p>	
<p>Recommendations: No further recommendations at this time.</p>	

<p>C Fully Compliant</p>	<p>Evidence: SR-Third Party Risk Management Policy</p>
<p>Regulation: (c) Whether a business conducts due diligence of its service providers and contractors factors into whether the business has reason to believe that a service provider or contractor is using personal information in violation of the CCPA and these regulations.</p>	
<p>Observations/Findings: Thoropass performs due diligence on all service providers and contracts to ensure personal information is not being used in violation of the CCPA.</p>	
<p>Recommendations: No further recommendations at this time.</p>	

7052 Third Parties

<p>A Not Applicable</p>	<p>Evidence: N/A</p>
<p>Regulation: (a) A third party that does not have a contract that complies with section 7053, subsection (a), shall not collect, use, process, retain, sell, or share the personal information that the business made available to it.</p>	
<p>Observations/Findings: N/A. Thoropass does not work with any third-parties not considered service providers or contractors. All service providers, contractors, or other organizations Thoropass works with are under a contract (such as a Non-Disclosure Agreement) restricting the collection, use, processing, selling, or sharing of consumers' personal information (considered confidential or sensitive information) of Thoropass.</p>	

Recommendations: Not applicable.

B Fully Compliant **Evidence:** Non-Disclosure Agreements; Other Contracts

Regulation:

(b) A third party shall comply with the terms of the contract required by the CCPA and these regulations, which include treating the personal information that the business made available to it in a manner consistent with the business’s obligations under the CCPA and these regulations.

Observations/Findings: All service providers, contractors, and third parties must comply with the terms of contract between them and Thoropass as well as required to meet CCPA regulations to include treating personal information in a manner consistent with Thoropass's obligation under the CCPA.

Recommendations: No further recommendations at this time.

7053 Contract Requirements for Third Parties

A Fully Compliant **Evidence:** SR-Third Party Risk Management Procedures; Contract Review

Regulation:

(a) A business that sells or shares a consumer’s personal information with a third party shall enter into an agreement with the third party that:

- (1) Identifies the limited and specified purpose(s) for which the personal information is made available to the third party. The purpose(s) shall not be described in generic terms, such as referencing the entire contract generally. The description shall be specific.
- (2) Specifies that the business is making the personal information available to the third party only for the limited and specified purpose(s) set forth within the contract and requires the third party to use it only for that limited and specified purpose(s).
- (3) Requires the third party to comply with all applicable sections of the CCPA and these regulations, including—with respect to the personal information that the business makes available to the third party—providing the same level of privacy protection as required of businesses by the CCPA and these regulations.
- (4) Grants the business the right—with respect to the personal information that the business makes available to the third party—to take reasonable and appropriate steps to ensure that the third party uses it in a manner consistent with the business’s obligations under the CCPA and these regulations.
- (5) Grants the business the right, upon notice, to take reasonable and appropriate steps to stop and remediate unauthorized use of personal information made available to the third party.
- (6) Requires the third party to notify the business after it makes a determination that it can no longer meet its obligations under the CCPA and these regulations.

Observations/Findings: Thoropass performs contract reviews to ensure service providers and contractors of Thoropass meet the requirements of CCPA to include:

- Limited and Specified Business Purposes: Ensure contract identifies specific business purposes for which personal information is being processed and specify information is disclosed only for the limited/specified business purpose(s). Ensure description is specific.
- Require Compliance with the CCPA and provide same level of Privacy Protection: Ensure contract requires compliance with all applicable sections of the CCPA and provide for the same level of privacy protection as required by the CCPA
- Grant Right to Review: Ensure contract provides for the right to take reasonable and appropriate steps to ensure compliance with CCPA (to include ongoing manual reviews, automated scans, internal/third-party assessments, audits, or other technical/operational

<p>testing at least once every twelve (12) months).</p> <ul style="list-style-type: none"> • Right to Stop/Remediate Unauthorized Use: Ensure contract provides for the right, upon notice, to take reasonable and appropriate steps to stop and remediate any unauthorized use of personal information to include providing documentation verifying personal information is no longer retained or used once a valid request to delete was made. • Notification: Ensure contract requires notification after a determination is made service provider/contractor can no longer meet CCPA obligations/requirements.
<p>Recommendations: No further recommendations at this time.</p>

<p>B Fully Compliant</p>	<p>Evidence: SR-Third Party Risk Management Policy</p>
<p>Regulation: (b) Whether a business conducts due diligence of the third party factors into whether the business has reason to believe that the third party is using personal information in violation of the CCPA and these regulations.</p>	
<p>Observations/Findings: All service providers, contractors, and third parties must comply with the terms of contract between them and Thoropass as well as required to meet CCPA regulations to include treating personal information in a manner consistent with Thoropass's obligation under the CCPA.</p>	
<p>Recommendations: No further recommendations at this time.</p>	

Article 5 Verification of Requests

7060 General Rules Regarding Verification

<p>A Fully Compliant</p>	<p>Evidence: PT-02 Authority to Process PII</p>
<p>Regulation: (a) A business shall establish, document, and comply with a reasonable method for verifying that the person making a request to delete, request to correct, or request to know is the consumer about whom the business has collected information.</p>	
<p>Observations/Findings: Thoropass will establish, document, and comply with a reasonable method to verify a person's identity making a request to delete, correct, or know. <i>Note: Thoropass has not received any CCPA related requests from any consumers over the last twelve (12) months.</i></p>	
<p>Recommendations: No further recommendations at this time.</p>	

<p>B Not Applicable</p>	<p>Evidence: N/A</p>
<p>Regulation: (b) A business shall not require a consumer to verify their identity to make a request to opt-out of sale/sharing or to make a request to limit. A business may ask the consumer for information necessary to complete the request; however, it shall not be burdensome on the consumer.</p>	
<p>Observations/Findings: N/A. Thoropass does not sell or share personal information and is not</p>	

required to provide for a request to opt-out of sale/sharing.

Recommendations: Not applicable.

C Fully Compliant

Evidence: PT-02 Authority to Process PII

Regulation:

(c) In determining the method by which the business will verify the consumer's identity, the business shall:

(1) Whenever feasible, match the identifying information provided by the consumer to the personal information of the consumer already maintained by the business, or use a third-party identity verification service that complies with this section.

(2) Avoid collecting the types of personal information identified in Civil Code section 1798.81.5, subdivision (d), unless necessary for the purpose of verifying the consumer.

(3) Consider the following factors:

(A) The type, sensitivity, and value of the personal information collected and maintained about the consumer. Sensitive personal information shall warrant a more stringent verification process.

(B) The risk of harm to the consumer posed by any unauthorized deletion, correction, or access. A greater risk of harm to the consumer by unauthorized deletion, correction, or access shall warrant a more stringent verification process.;

(C) The likelihood that fraudulent or malicious actors would seek the personal information. The higher the likelihood, the more stringent the verification process shall be.;

(D) Whether the personal information to be provided by the consumer to verify their identity is sufficiently robust to protect against fraudulent requests or being spoofed or fabricated.;

(E) The manner in which the business interacts with the consumer.

(F) Available technology for verification.

Observations/Findings: Thoropass will:

- Whenever feasible, match the identifying information provided by the consumer to the personal information of the consumer already maintained by Thoropass, or use a third-party identity verification service.
- Avoid collecting the following types of personal information, unless necessary for the purpose of verifying the consumer:
 - Personal information
 - Individuals first name (or first initial) and individual's last name in combination with any one or more of the following:
 - Social security number
 - Driver's license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual.
 - Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.
 - Medical information.
 - Health insurance information.
 - Unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual. Unique biometric data does not include a physical or digital photograph, unless used or stored for facial recognition purposes.
 - Genetic data.
 - A username or email address in combination with a password or security question and answer that would permit access to an online account.

Consider the following factors:

- The type, sensitivity, and value of the personal information collected and maintained about the consumer. Sensitive or valuable personal information shall warrant a more stringent verification process. The types of personal information identified in above, shall be considered presumptively sensitive;
- The risk of harm to the consumer posed by any unauthorized access or deletion. A greater risk of harm to the consumer by unauthorized access or deletion shall warrant a more stringent verification process;
- The likelihood that fraudulent or malicious actors would seek the personal information. The higher the likelihood, the more stringent the verification process shall be;
- Whether the personal information to be provided by the consumer to verify their identity is sufficiently robust to protect against fraudulent requests or being spoofed or fabricated;
- The manner in which the business interacts with the consumer; and
- Available technology for verification.

Note: Thoropass has not received any CCPA related requests from any consumers over the last twelve (12) months.

Recommendations: No further recommendations at this time.

D Fully Compliant

Evidence: PT-02 Authority to Process PII

Regulation:

(d) A business shall generally avoid requesting additional information from the consumer for purposes of verification. If, however, the business cannot verify the identity of the consumer from the information already maintained by the business, the business may request additional information from the consumer, which shall only be used for the purposes of verifying the identity of the consumer seeking to exercise their rights under the CCPA, security, or fraud-prevention. The business shall delete any new personal information collected for the purposes of verification as soon as practical after processing the consumer's request, except as required to comply with section 7101.

Observations/Findings: Thoropass will generally avoid requesting additional information from the consumer for purposes of verification; however, if Thoropass cannot verify the identity of the consumer from the information already maintained by Thoropass, Thoropass may request additional information from the consumer, which shall only be used for the purposes of verifying the identity of the consumer seeking to exercise their rights under the CCPA, security, or fraud-prevention. Thoropass will delete any new personal information collected for the purposes of verification as soon as practical after processing the consumer's request, except as required to comply with CCPA regulations.

Note: Thoropass has not received any CCPA related requests from any consumers over the last twelve (12) months.

Recommendations: No further recommendations at this time.

E Fully Compliant

Evidence: PT-02 Authority to Process PII

Regulation:

(e) A business shall not require the consumer or the consumer's authorized agent to pay a fee for the verification of their request to delete, request to correct, or request to know. For example, a business may not require a consumer to provide a notarized affidavit to verify their identity unless the business compensates the consumer for the cost of notarization.

Observations/Findings: Thoropass will not require the consumer (or the consumer's authorized agent) to pay a fee for the verification of their request to know or request to delete. For example, Thoropass will not require a consumer to provide a notarized affidavit to verify their identity unless Thoropass compensates the consumer for the cost of notarization.

Note: Thoropass has not received any CCPA related requests from any consumers over the last twelve (12) months.

Recommendations: No further recommendations at this time.

F Fully Compliant

Evidence: PT-02 Authority to Process PII

Regulation:

(f) A business shall implement reasonable security measures to detect fraudulent identity- verification activity and prevent the unauthorized deletion, correction, or access of a consumer's personal information.

Observations/Findings: Thoropass will implement reasonable security measures to detect fraudulent identity-verification activity and prevent the unauthorized access to or deletion of a consumer's personal information. *Note: Thoropass has not received any CCPA related requests from any consumers over the last twelve (12) months.*

Recommendations: No further recommendations at this time.

G Fully Compliant

Evidence: PT-02 Authority to Process PII

Regulation:

(g) If a business maintains consumer information that is deidentified, a business is not obligated to provide or delete this information in response to a consumer request or to re- identify individual data to verify a consumer request.

Observations/Findings: If Thoropass maintains consumer information that is deidentified, Thoropass is not obligated to provide (or delete) this information in response to a consumer request or to re-identify individual data to verify a consumer request.

Recommendations: No further recommendations at this time.

H Fully Compliant

Evidence: PT-02 Authority to Process PII

Regulation:

(h) For requests to correct, the business shall make an effort to verify the consumer based on personal information that is not the subject of the request to correct.

Observations/Findings: For requests to correct, Thoropass will make an effort to verify the consumer based on personal information that is not the subject of the request to correct. *Note: Thoropass has not received any CCPA related requests from any consumers over the last twelve (12) months.*

Recommendations: No further recommendations at this time.

7061 Verification for Password-Protected Accounts

A Fully Compliant	Evidence: PT-02 Authority to Process PII
Regulation: (a) If a business maintains a password-protected account with the consumer, the business may verify the consumer's identity through the business's existing authentication practices for the consumer's account, provided that the business follows the requirements in section 7060. The business shall also require a consumer to re-authenticate themselves before deleting, correcting, or disclosing the consumer's data.	
Observations/Findings: If Thoropass maintains a password-protected account with the consumer, Thoropass will verify the consumer's identity through Thoropass's existing authentication practices for the consumer's account, provided that Thoropass follows the requirements in the CCPA regulations and uses reasonable data security controls. Thoropass will also require a consumer to re-authenticate themselves before disclosing or deleting the consumer's data.	
Recommendations: No further recommendations at this time.	

B Fully Compliant	Evidence: PT-02 Authority to Process PII
Regulation: (b) If a business suspects fraudulent or malicious activity on or from the password-protected account, the business shall not comply with a consumer's request to delete, request to correct, or request to know until further verification procedures determine that the consumer request is authentic and the consumer making the request is the person about whom the business has collected information. The business may use the procedures set forth in section 7062 to further verify the identity of the consumer.	
Observations/Findings: If Thoropass suspects fraudulent or malicious activity on or from the password-protected account, Thoropass will not comply with a consumer's request to know or request to delete until further verification procedures determine that the consumer request is authentic and the consumer making the request is the person about whom the business has collected information. Thoropass may use the above procedures to further verify the identity of the consumer.	
Recommendations: No further recommendations at this time.	

7062 Verification for Non-Accountholders

A Fully Compliant	Evidence: PT-02 Authority to Process PII
Regulation: (a) If a consumer does not have or cannot access a password-protected account with a business, the business shall comply with this section, in addition to section 7060.	
Observations/Findings: If a consumer does not have or cannot access a password-protected account with Thoropass, Thoropass will comply with section 7060 of the CCPA regarding verification for non-account holders.	
Recommendations: No further recommendations at this time.	

B Fully Compliant**Evidence:** PT-02 Authority to Process PII**Regulation:**

(b) A business's compliance with a request to know categories of personal information requires that the business verify the identity of the consumer making the request to a reasonable degree of certainty. A reasonable degree of certainty may include matching at least two data points provided by the consumer with data points maintained by the business that it has determined to be reliable for the purpose of verifying the consumer.

Observations/Findings: Thoropass's compliance with a request to know categories of personal information requires Thoropass to verify the identity of the consumer making the request to a reasonable degree of certainty. *Note: A reasonable degree of certainty may include matching at least two (2) data points provided by the consumer with data points maintained by Thoropass that it has determined to be reliable for the purpose of verifying the consumer.*

Recommendations: No further recommendations at this time.

C Fully Compliant**Evidence:** PT-02 Authority to Process PII**Regulation:**

(c) A business's compliance with a request to know specific pieces of personal information requires that the business verify the identity of the consumer making the request to a reasonably high degree of certainty. A reasonably high degree of certainty may include matching at least three pieces of personal information provided by the consumer with personal information maintained by the business that it has determined to be reliable for the purpose of verifying the consumer together with a signed declaration under penalty of perjury that the requestor is the consumer whose personal information is the subject of the request. If a business uses this method for verification, the business shall maintain all signed declarations as part of its record-keeping obligations.

Observations/Findings: Thoropass's compliance with a request to know specific pieces of personal information requires Thoropass to verify the identity of the consumer making the request to a reasonably high degree of certainty. *Note: A reasonably high degree of certainty may include matching at least three (3) pieces of personal information provided by the consumer with personal information maintained by Thoropass that it has determined to be reliable for the purpose of verifying the consumer together with a signed declaration under penalty of perjury that the requestor is the consumer whose personal information is the subject of the request. If Thoropass uses this method for verification, Thoropass will maintain all signed declarations as part of its record-keeping obligations. Note: Thoropass has not received any CCPA related requests from any consumers over the last twelve (12) months.*

Recommendations: No further recommendations at this time.

D Fully Compliant**Evidence:** PT-02 Authority to Process PII**Regulation:**

(d) A business's compliance with a request to delete or a request to correct may require that the business verify the identity of the consumer to a reasonable or reasonably high degree of certainty depending on the sensitivity of the personal information and the risk of harm to the consumer posed by unauthorized deletion or correction. For example, the deletion of family photographs or the correction of contact information may require a reasonably high degree of certainty, while the deletion of browsing history or correction of marital status may require only a reasonable degree of certainty. A business shall act in good faith when determining the appropriate standard to apply when verifying the consumer

in accordance with these regulations.

Observations/Findings: Thoropass's compliance with a request to delete may require Thoropass to verify the identity of the consumer to a reasonable or reasonably high degree of certainty depending on the sensitivity of the personal information and the risk of harm to the consumer posed by unauthorized deletion. Thoropass will act in good faith when determining the appropriate standard to apply when verifying the consumer in accordance with these regulations. *Note: Thoropass has not received any CCPA related requests from any consumers over the last twelve (12) months.*

Recommendations: No further recommendations at this time.

E Not Applicable

Evidence: N/A

Regulation:

(e) Illustrative examples follow:

(1) Example 1: If a business maintains personal information in a manner associated with a named actual person, the business may verify the consumer by requiring the consumer to provide evidence that matches the personal information maintained by the business. For example, if a retailer maintains a record of purchases made by a consumer, the business may require the consumer to identify items that they recently purchased from the store or the dollar amount of their most recent purchase to verify their identity to a reasonable degree of certainty.

(2) Example 2: If a business maintains personal information in a manner that is not associated with a named actual person, the business may verify the consumer by requiring the consumer to demonstrate that they are the sole consumer associated with the personal information. For example, a business may have a mobile application that collects personal information about the consumer but does not require an account. The business may determine whether, based on the facts and considering the factors set forth in section 7060, subsection (b)(3), it may reasonably verify a consumer by asking them to provide information that only the person who used the mobile application may know or by requiring the consumer to respond to a notification sent to their device.

Observations/Findings: N/A. These are illustrative examples.

Recommendations: Not applicable.

F Fully Compliant

Evidence: PT-02 Authority to Process PII

Regulation:

(f) A business shall deny a request to know specific pieces of personal information if it cannot verify the identity of the requestor pursuant to these regulations.

Observations/Findings: Thoropass will deny a request to know specific pieces of personal information if it cannot verify the identity of the requestor pursuant to the CCPA regulations. *Note: Thoropass has not received any CCPA related requests from any consumers over the last twelve (12) months.*

Recommendations: No further recommendations at this time.

G Fully Compliant

Evidence: PT-02 Authority to Process PII

Regulation:

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

Observations/Findings: If there is no reasonable method by which Thoropass can verify the identity of the consumer to the degree of certainty required by CCPA, Thoropass shall state so in response to any request and explain why it has no reasonable method by which it can verify the identity of the requestor. If Thoropass has no reasonable method by which it can verify any consumer, Thoropass shall explain why it has no reasonable verification method in its privacy policy. Thoropass shall evaluate and document whether a reasonable method can be established at least once every twelve (12) months, in connection with the requirement to update its privacy policy.

Recommendations: No further recommendations at this time.

7063 Authorized Agents

A Fully Compliant Evidence: PT-02 Authority to Process PII

Regulation:

(a) When a consumer uses an authorized agent to submit a request to delete, request to correct, or a request to know, a business may require the authorized agent to provide proof that the consumer gave the agent signed permission to submit the request. The business may also require the consumer to do either of the following:

- (1) Verify their own identity directly with the business.
- (2) Directly confirm with the business that they provided the authorized agent permission to submit the request.

Observations/Findings: When a consumer uses an authorized agent to submit a request to know request to correct, or a request to delete, Thoropass will require the authorized agent to provide proof that the consumer gave the agent signed permission to submit the request. Thoropass will also require the consumer to do either of the following:

- Verify their own identity directly with Thoropass.
- Directly confirm with Thoropass that they provided the authorized agent permission to submit the request.

Note: Thoropass has not received any CCPA related requests from any consumers over the last twelve (12) months.

Recommendations: No further recommendations at this time.

B Fully Compliant Evidence: PT-02 Authority to Process PII

Regulation:

(b) Subsection (a) does not apply when a consumer has provided the authorized agent with power of attorney pursuant to Probate Code sections 4121 to 4130. A business shall not require power of attorney in order for a consumer to use an authorized agent to act on their behalf.

Observations/Findings: These requirements do not apply when a consumer has provided the

authorized agent with power of attorney.

Recommendations: No further recommendations at this time.

C Fully Compliant **Evidence:** PT-02 Authority to Process PII

Regulation:

(c) An authorized agent shall implement and maintain reasonable security procedures and practices to protect the consumer's information.

Observations/Findings: Thoropass requires an authorized agent to implement and maintain reasonable security procedures and practices to protect the consumer's information.

Recommendations: No further recommendations at this time.

D Fully Compliant **Evidence:** PT-02 Authority to Process PII

Regulation:

(d) An authorized agent shall not use a consumer's personal information, or any information collected from or about the consumer, for any purposes other than to fulfill the consumer's requests, verification, or fraud prevention.

Observations/Findings: Thoropass requires an authorized agent to not use a consumer's personal information, or any information collected from or about the consumer, for any purposes other than to fulfill the consumer's requests, verification, or fraud prevention.

Recommendations: No further recommendations at this time.

Article 6 Special Rules Regarding Consumers Under 16 Years of Age

7070 Consumers Less Than 13 Years of Age

A Not Applicable **Evidence:** N/A

Regulation:

(a) Process for Opting-In to Sale or Sharing of Personal Information

(1) A business that has actual knowledge that it sells or shares the personal information of a consumer less than the age of 13 shall establish, document, and comply with a reasonable method for determining that the person consenting to the sale or sharing of the personal information about the child is the parent or guardian of that child. This consent to the sale or sharing of personal information is in addition to any verifiable parental consent required under COPPA.

(2) Methods that are reasonably calculated to ensure that the person providing consent is the child's parent or guardian include, but are not limited to:

(A) Providing a consent form to be signed by the parent or guardian under penalty of perjury and returned to the business by postal mail, facsimile, or electronic scan;

(B) Requiring a parent or guardian, in connection with a monetary transaction, to use a credit card,

debit card, or other online payment system that provides notification of each discrete transaction to the primary account holder;

(C) Having a parent or guardian call a toll-free telephone number staffed by trained personnel;

(D) Having a parent or guardian connect to trained personnel via video-conference;

(E) Having a parent or guardian communicate in person with trained personnel; and

(F) Verifying a parent or guardian's identity by checking a form of government- issued identification against databases of such information, as long as the parent or guardian's identification is deleted by the business from its records promptly after such verification is complete.

Observations/Findings: N/A. Thoropass's services are not intended for or being sold to consumers under the age of thirteen (13).

Recommendations: Not applicable.

B Not Applicable

Evidence: N/A

Regulation:

(b) When a business receives consent to the sale or sharing of personal information pursuant to subsection (a), the business shall inform the parent or guardian of the right to opt-out of sale/sharing and of the process for doing so on behalf of their child pursuant to section 7026, subsections (a)-(f).

Observations/Findings: N/A. Thoropass's services are not intended for or being sold to consumers under the age of thirteen (13).

Recommendations: Not applicable.

C Not Applicable

Evidence: N/A

Regulation:

(c) A business shall establish, document, and comply with a reasonable method, in accordance with the methods set forth in subsection (a)(2), for determining that a person submitting a request to delete, request to correct, or request to know the personal information of a child under the age of 13 is the parent or guardian of that child.

Observations/Findings: N/A. Thoropass's services are not intended for or being sold to consumers under the age of thirteen (13).

Recommendations: Not applicable.

7071 Consumers at Least 13 Years of Age and Less Than 16 Years of Age

A Not Applicable

Evidence: N/A

Regulation:

(a) A business that has actual knowledge that it sells or shares the personal information of consumers at least 13 years of age and less than 16 years of age shall establish, document, and comply with a reasonable process for allowing such consumers to opt-in to the sale or sharing of their personal information, pursuant to section 7028.

Observations/Findings: N/A. Thoropass's services are not intended for or being sold to consumers

at least thirteen (13) years of age and less than sixteen (16) years of age.

Recommendations: Not applicable.

B Not Applicable

Evidence: N/A

Regulation:

(b) When a business receives a request to opt-in to the sale or sharing of personal information from a consumer at least 13 years of age and less than 16 years of age, the business shall inform the consumer of their ongoing right to opt-out of sale/sharing at any point in the future and of the process for doing so pursuant to section 7026.

Observations/Findings: N/A. Thoropass's services are not intended for or being sold to consumers at least thirteen (13) years of age and less than sixteen (16) years of age.

Recommendations: Not applicable.

7072 Notices to Consumers Less Than 16 Years of Age

A Not Applicable

Evidence: N/A

Regulation:

(a) A business subject to sections 7070 and/or 7071 shall include a description of the processes set forth in those sections in its privacy policy.

Observations/Findings: N/A. Thoropass's services are not intended for or being sold to consumers less than sixteen (16) years of age.

Recommendations: Not applicable.

B Not Applicable

Evidence: N/A

Regulation:

(b) A business that exclusively targets offers of goods or services directly to consumers under 16 years of age and does not sell or share the personal information without the consent of consumers at least 13 years of age and less than 16 years of age, or the consent of their parent or guardian for consumers under 13 years of age, is not required to provide the Notice of Right to Opt-out of Sale/Sharing.

Observations/Findings: N/A. Thoropass's services are not intended for or being sold to consumers less than sixteen (16) years of age.

Recommendations: Not applicable.

Article 7 Non-Discrimination

7080 Discriminatory Practices

A Fully Compliant	Evidence: PT-05 Privacy Notice
Regulation: (a) A price or service difference is discriminatory, and therefore prohibited by Civil Code section 1798.125, if the business treats a consumer differently because the consumer exercised a right conferred by the CCPA or these regulations.	
Observations/Findings: Thoropass recognizes a financial incentive or a price or service difference is discriminatory, and therefore prohibited by the CCPA, if Thoropass treats a consumer differently because the consumer exercised a right conferred by the CCPA regulations.	
Recommendations: No further recommendations at this time.	

B Fully Compliant	Evidence: PT-05 Privacy Notice
Regulation: (b) A business may offer a price or service difference that is non-discriminatory. A price or service difference is non-discriminatory if it is reasonably related to the value of the consumer's data. If a business is unable to calculate a good-faith estimate of the value of the consumer's data or cannot show that the price or service difference is reasonably related to the value of the consumer's data, that business shall not offer the price or service difference.	
Observations/Findings: Thoropass is not prohibited from charging an individual a different price or rate, or from providing a different level or quality of goods or services to the individual, if that difference is reasonably related to the value provided to Thoropass by the individual's data. Thoropass is not prohibited from offering loyalty, rewards, premium features, discounts, or club card programs consistent with the regulations. Thoropass does not offer a financial incentive or price/service difference, but may offer a financial incentive or price or service difference if it is reasonably related to the value of the consumer's data. If Thoropass is unable to calculate a good-faith estimate of the value of the consumer's data or cannot show that the financial incentive or price or service difference is reasonably related to the value of the consumer's data, Thoropass will not offer the financial incentive or price or service difference.	
Recommendations: No further recommendations at this time.	

C Fully Compliant	Evidence: PT-05 Privacy Notice
Regulation: (c) A business's denial of a consumer's request to delete, request to correct, request to know, or request to opt-out of sale/sharing for reasons permitted by the CCPA or these regulations shall not be considered discriminatory.	
Observations/Findings: Thoropass recognizes its denial of a consumer's request to know, request to delete, or request to opt-out for reasons permitted by the CCPA regulations will not be considered discriminatory.	

Recommendations: No further recommendations at this time.

D Not Applicable

Evidence: N/A

Regulation:

(d) Illustrative examples follow:

(1) Example 1: A music streaming business offers a free service as well as a premium service that costs \$5 per month. If only the consumers who pay for the music streaming service are allowed to opt-out of the sale or sharing of their personal information, then the practice is discriminatory, unless the \$5-per-month payment is reasonably related to the value of the consumer's data to the business.

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

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

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

Observations/Findings: N/A. Illustrative examples.

Recommendations: Not applicable.

E Not Applicable

Evidence: N/A

Regulation:

(e) A business shall notify consumers of any financial incentive or price or service difference subject to Civil Code section 1798.125 that it offers in accordance with section 7016.

Observations/Findings: N/A. Thoropass does not provide any financial incentive or price/service differences.

Recommendations: Not applicable.

F Fully Compliant	Evidence: PT-05 Privacy Notice
Regulation: (f) A business's charging of a reasonable fee pursuant to Civil Code section 1798.145, subdivision (h)(3), shall not be considered a financial incentive subject to these regulations.	
Observations/Findings: Thoropass recognizes its charging of a reasonable fee pursuant to CCPA will not be considered a financial incentive subject to the CCPA regulations.	
Recommendations: No further recommendations at this time.	

G Fully Compliant	Evidence: PT-05 Privacy Notice
Regulation: (g) A price or service difference that is the direct result of compliance with a state or federal law shall not be considered discriminatory.	
Observations/Findings: Thoropass recognizes a price or service difference that is the direct result of compliance with a state or federal law will not be considered discriminatory.	
Recommendations: No further recommendations at this time.	

7081 Calculating the Value of Consumer Data

A Fully Compliant	Evidence: PT-05 Privacy Notice
Regulation: (a) A business offering a price or service difference subject to Civil Code section 1798.125 shall use and document a reasonable and good -faith method for calculating the value of the consumer's data. The business shall consider one or more of the following: <ol style="list-style-type: none"> (1) The marginal value to the business of the sale, collection, or deletion of a consumer's data. (2) The average value to the business of the sale, collection, or deletion of a consumer's data. (3) The aggregate value to the business of the sale, collection, or deletion of consumers' data divided by the total number of consumers. (4) Revenue generated by the business from sale, collection, or retention of consumers' personal information. (5) Expenses related to the sale, collection, or retention of consumers' personal information. (6) Expenses related to the offer, provision, or imposition of any financial incentive or price or service difference. (7) Profit generated by the business from sale, collection, or retention of consumers' personal information. (8) Any other practical and reasonably reliable method of calculation used in good faith. 	
Observations/Findings: Thoropass does not offer a financial incentive; however, Thoropass recognizes by offering a financial incentive or price or service difference subject to the CCPA, it will use and document a reasonable and good faith method for calculating the value of the consumer's data. Thoropass will consider one or more of the following: <ul style="list-style-type: none"> • The marginal value to the business of the sale, collection, or deletion of a consumer's data. • The average value to the business of the sale, collection, or deletion of a consumer's data. • The aggregate value to the business of the sale, collection, or deletion of consumers' data divided by the total number of consumers. • Revenue generated by the business from sale, collection, or retention of consumers' personal 	

<p>information.</p> <ul style="list-style-type: none"> • Expenses related to the sale, collection, or retention of consumers' personal information. • Expenses related to the offer, provision, or imposition of any financial incentive or price or service difference. • Profit generated by the business from sale, collection, or retention of consumers' personal information. • Any other practical and reasonably reliable method of calculation used in good faith.
<p>Recommendations: No further recommendations at this time.</p>

<p>B Fully Compliant</p>	<p>Evidence: PT-05 Privacy Notice</p>
<p>Regulation: (b) For the purpose of calculating the value of consumer data, a business may consider the value to the business of the data of all natural persons in the United States and not just consumers.</p>	
<p>Observations/Findings: For the purpose of calculating the value of consumer data, Thoropass may consider the value to Thoropass of the data of all natural persons in the United States and not just consumers. <i>Note: Thoropass does not provide financial incentives.</i></p>	
<p>Recommendations: No further recommendations at this time.</p>	

Article 8 Training and Record-Keeping

7100 Training

<p>A Fully Compliant</p>	<p>Evidence: AT-03 Awareness and Training Policy</p>
<p>Regulation: (a) All individuals responsible for handling consumer inquiries about the business's information practices or the business's compliance with the CCPA shall be informed of all of the requirements in the CCPA and these regulations and how to direct consumers to exercise their rights under the CCPA and these regulations.</p>	
<p>Observations/Findings: Thoropass informs all employees responsible for handling consumer inquiries about the organization's privacy practices and/or the organization's compliance with California Consumer Privacy Act (CCPA) regulations. Thoropass also informs consumers on how to exercise their rights under the CCPA regulations.</p> <p>Training covers:</p> <ul style="list-style-type: none"> • Using reasonable protection measures to secure consumer request records; • Following procedures for maintaining a ticket (or log) including: the date and nature of the request, the manner in which the request was made, the date and nature of the organization's response, and, if the request was denied, the basis for the denial (in whole or in part) Note: The maintenance of these records alone does not violate CCPA regulations. • Understanding acceptable purposes for maintaining information for record-keeping, which are only as necessary in order to be reviewed in compliance with CCPA regulations and which exclude sharing with third parties except as may be required by law; and • Understanding Thoropass is not required to retain personal information solely for the purpose of fulfilling consumer requests made under CCPA. 	

Training related to security awareness and privacy (i.e. CCPA), is provided within sixty (60) days of onboarding and annually thereafter. Training is distributed and tracked through Thoropass's learning management system (LMS). *Note: Currently only the Data Protection Officer handles consumers' requests. Thoropass has not received any CCPA related requests from any consumers over the last twelve (12) months.*

Recommendations: No recommendations at this time.

B Not Applicable

Evidence: N/A

Regulation:

(b) A business that knows or reasonably should know that it, alone or in combination, buys, receives for the business's commercial purposes, sells, or shares for commercial purposes the personal information of 10,000,000 or more consumers in a calendar year shall establish, document, and comply with a training policy to ensure that all individuals responsible for handling consumer requests made under the CCPA or the business's compliance with the CCPA are informed of all the requirements in these regulations and the CCPA.

Observations/Findings: N/A. Thoropass does not buy, receive, sell, or share personal information of ten (10) million or more consumers in a calendar year.

Recommendations: Not applicable.

7101 Record-Keeping

A Fully Compliant

Evidence: AT-03 Awareness and Training Policy

Regulation:

(a) A business shall maintain records of consumer requests made pursuant to the CCPA and how it responded to the requests for at least 24 months. The business shall implement and maintain reasonable security procedures and practices in maintaining these records.

Observations/Findings: Thoropass will train employees to maintain records of consumer requests made under the CCPA and responses to these requests for at least twenty-four (24) months. *Note: Thoropass has not received any CCPA related requests from any consumers over the last twelve (12) months.*

Recommendations: No further recommendations at this time.

B Fully Compliant

Evidence: LISD Ticketing Solution (Jira)

Regulation:

(b) The records may be maintained in a ticket or log format provided that the ticket or log includes the date of request, nature of request, manner in which the request was made, the date of the business's response, the nature of the response, and the basis for the denial of the request if the request is denied in whole or in part.

Observations/Findings: Thoropass will maintain tickets of requests within Jira containing date of request, nature of request, manner request was made, date of response, nature of response, and basis of denial if request is denied. *Note: Thoropass has not received any CCPA related requests from any*

consumers over the last twelve (12) months.

Recommendations: No further recommendations at this time.

C Fully Compliant **Evidence:** PT-02 Authority to Process PII

Regulation:

(c) A business's maintenance of the information required by this section, where that information is not used for any other purpose, does not taken alone violate the CCPA or these regulations.

Observations/Findings: Thoropass recognizes the maintenance of this information not used for any other purpose does not violate the CCPA.

Recommendations: No further recommendations at this time.

D Fully Compliant **Evidence:** PT-02 Authority to Process PII

Regulation:

(d) Information maintained for record-keeping purposes shall not be used for any other purpose except as reasonably necessary for the business to review and modify its processes for compliance with the CCPA and these regulations. Information maintained for record- keeping purposes shall not be shared with any third party except as necessary to comply with a legal obligation.

Observations/Findings: Thoropass does not use the information maintained for record-keeping purposes for any other purpose except as reasonably necessary for review and modification to comply with CCPA. Information maintained for record-keeping purposes is not shared with any third-party except as legally required.

Recommendations: No further recommendations at this time.

E Fully Compliant **Evidence:** PT-02 Authority to Process PII

Regulation:

(e) Other than as required by subsection (b), a business is not required to retain personal information solely for the purpose of fulfilling a consumer request made under the CCPA.

Observations/Findings: Thoropass is not required to retain personal information solely for the purpose of fulfilling a consumer request made under the CCPA.

Recommendations: No further recommendations at this time.

7102 Requirements for Businesses Collecting Large Amounts of Personal Information

A Not Applicable **Evidence:** N/A

Regulation:

(a) A business that knows or reasonably should know that it, alone or in combination, buys, receives for

the business's commercial purposes, sells, shares, or otherwise makes available for commercial purposes the personal information of 10,000,000 or more consumers in a calendar year shall:

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

- (A) The number of requests to delete that the business received, complied with in whole or in part, and denied;
- (B) The number of requests to correct that the business received, complied with in whole or in part, and denied;
- (C) The number of requests to know that the business received, complied with in whole or in part, and denied;
- (D) The number of requests to opt-out of sale/sharing that the business received, complied with in whole or in part, and denied;
- (E) The number of requests to limit that the business received, complied with in whole or in part, and denied; and
- (F) The median or mean number of days within which the business substantively responded to requests to delete, requests to correct, requests to know, requests to opt-out of sale/sharing, and requests to limit.

(2) Disclose, by July 1 of every calendar year, the information compiled in subsection (a)(1) within their privacy policy or posted on their website and accessible from a link included in their privacy policy. In its disclosure, a business may choose to disclose the number of requests that it denied in whole or in part because the request was not verifiable, was not made by a consumer, called for information exempt from disclosure, or was denied on other grounds.

Observations/Findings: N/A. Thoropass does not buy, receive, sell, or share personal information of ten (10) million or more consumers in a calendar year.

Recommendations: Not applicable.

B Not Applicable	Evidence: N/A
<p>Regulation: (b) A business may choose to compile and disclose the information required by subsection (a)(1) for requests received from all individuals, rather than requests received from consumers. The business shall state whether it has done so in its disclosure and shall, upon request, compile and provide to the Attorney General the information required by subsection (a)(1) for requests received from consumers.</p>	
<p>Observations/Findings: N/A. Thoropass does not buy, receive, sell, or share personal information of ten (10) million or more consumers in a calendar year.</p>	
<p>Recommendations: Not applicable.</p>	

Article 9 Investigation and Enforcement

7300 Sworn Complaints Filed with the Agency

Not Applicable	Evidence: N/A
<p>Regulation: Sworn Complaints Filed with the Agency.</p>	

(a) Requirements for filing a sworn complaint. Sworn complaints may be filed with the Enforcement Division via the electronic complaint system available on the Agency’s website at <https://cppa.ca.gov/> or submitted in person or by mail to the headquarters office of the Agency.

A complaint must:

- (1) Identify the business, service provider, contractor, or person who allegedly violated the CCPA;
- (2) State the facts that support each alleged violation and include any documents or other evidence supporting this conclusion;
- (3) Authorize the alleged violator and the Agency to communicate regarding the complaint, including disclosing the complaint and any information relating to the complaint;
- (4) Include the name and current contact information of the complainant; and
- (5) Be signed and submitted under penalty of perjury.

(b) The Enforcement Division will notify the complainant in writing of the action, if any, the Agency has taken or plans to take on the complaint, together with the reasons for that action or nonaction.

Duplicate complaints submitted by the same complainant may be rejected without notice.

Observations/Findings: N/A. Article 9 is reserved for the CPPA.

Recommendations: Not applicable.

7301 Investigations

Not Applicable	Evidence: N/A
<p>Regulation: Investigations.</p> <p>(a) The Agency may open investigations upon the sworn complaint of any person or on its own initiative. For example, the Agency may initiate investigations based upon referrals from government agencies or private organizations, and non-sworn or anonymous complaints.</p> <p>(b) As part of the Agency’s decision to pursue investigations of possible or alleged violations of the CCPA, the Agency may consider all facts it determines to be relevant, including the amount of time between the effective date of the statutory or regulatory requirement(s) and the possible or alleged violation(s) of those requirements, and good-faith efforts to comply with those requirements.</p>	
<p>Observations/Findings: N/A. Article 9 is reserved for the CPPA.</p>	
<p>Recommendations: Not applicable.</p>	

7302 Probable Cause Proceedings

Not Applicable	Evidence: N/A
<p>Regulation: Probable Cause Proceedings.</p> <p>(a) Probable Cause. Under Civil Code section 1798.199.50, probable cause exists when the evidence supports a reasonable belief that the CCPA has been violated.</p> <p>(b) Probable Cause Notice. The Enforcement Division will provide the alleged violator with notice of the probable cause proceeding as required by Civil Code section 1798.199.50.</p> <p>(c) Probable Cause Proceeding.</p> <ul style="list-style-type: none"> (1) The proceeding shall be closed to the public unless the alleged violator files, at least 10 business days before the proceeding, a written request for a public proceeding. If the proceeding is not open to the public, then the proceeding may be conducted in whole or in part by telephone or videoconference. (2) The Agency shall conduct the proceeding informally. Only the alleged violator(s), their legal 	

counsel, and the Enforcement Division shall have the right to participate at the proceeding. The Agency shall determine whether there is probable cause based on the probable cause notice and any information or arguments presented at the probable cause proceeding by the parties.

(3) If the alleged violator(s) fails to participate or appear at the probable cause proceeding, the alleged violator(s) waives the right to further probable cause proceedings under Civil Code section 1798.199.50, and the Agency shall determine whether there is probable cause based on the notice and any information or arguments provided by the Enforcement Division.

(d) Probable Cause Determination. The Agency shall issue a written decision with its probable cause determination and serve it on the alleged violator electronically or by mail. The Agency's probable cause determination is final and not subject to appeal.

(e) Notices of probable cause and probable cause determinations shall not be open to the public nor admissible in evidence in any action or special proceeding other than one enforcing the CCPA.

Observations/Findings: N/A. Article 9 is reserved for the CPPA.

Recommendations: Not applicable.

7303 Stipulated Orders

Not Applicable	Evidence: N/A
<p>Regulation: Stipulated Orders.</p> <p>(a) At any time before or during an administrative hearing and in lieu of such a hearing, the Head of Enforcement and the alleged violator may stipulate to the entry of a final order. If a stipulation has been agreed upon and the scheduled date of the hearing is set to occur before the next Board meeting, the Enforcement Division will apply for a continuance of the hearing.</p> <p>(b) The final order must be approved by the Board, which may consider the matter in closed session.</p> <p>(c) The stipulated final order shall be public and have the force of an order of the Board.</p>	
<p>Observations/Findings: N/A. Article 9 is reserved for the CPPA.</p>	
<p>Recommendations: Not applicable.</p>	

7304 Agency Audits

Not Applicable	Evidence: N/A
<p>Regulation: Agency Audits.</p> <p>(a) Scope. The Agency may audit a business, service provider, contractor, or person to ensure compliance with any provision of the CCPA.</p> <p>(b) Criteria for Selection. The Agency may conduct an audit to investigate possible violations of the CCPA. Alternatively, the Agency may conduct an audit if the subject's collection or processing of personal information presents significant risk to consumer privacy or security, or if the subject has a history of noncompliance with the CCPA or any other privacy protection law.</p> <p>(c) Audits may be announced or unannounced as determined by the Agency.</p> <p>(d) Failure to Cooperate. A subject's failure to cooperate during the Agency's audit may result in the Agency issuing a subpoena, seeking a warrant, or otherwise exercising its powers to ensure compliance with the CCPA.</p> <p>(e) Protection of Personal Information. Consumer personal information disclosed to the Agency during an audit shall be maintained in compliance with the Information Practices Act of 1977, Civil Code</p>	

section 1798, et seq.

Observations/Findings: N/A. Article 9 is reserved for the CCPA.

Recommendations: Not applicable.

Appendices

Appendix A - Project Team

The following were the assigned Project Team Members during this assessment:

Thoropass	
Role	Team Member
Co-Founder/COO (Executive Management)	Eva Pittas
VP, Engineering (Approver)	Scott Schlegel
Data Protection Officer/CIOS (Assessor)	Jay Trinckes

Appendix B - List of Evidence Reviewed

The following was a list of documents reviewed during this assessment:

1. Evidence of Consent
2. Evidence of Contract Reviews
3. Evidence of deletion of personal information based on request (tickets for churn accounts; no consumer personal information requests have been received to date)
4. Evidence of methods to submit requests (online - privacy@thoropass.com)
5. Evidence of password-protected accounts (<https://app.thoropass.com>)
6. Evidence of process of verification (process in place, but no consumer personal information requests have been received to date)
7. Evidence of responding to requests (process in place, but no consumer personal information requests have been received to date)
8. Evidence of responses to requests (denial or approval) (process in place, but no consumer personal information requests have been received to date)
9. Data Protection Agreement (DPA)
10. Data Protection Impact Assessment (DPIA)
11. Non-Disclosure Agreements (other contracts)
12. Privacy Notice (<https://thoropass.com/privacy-policy>)
13. Privacy Policy and Procedures
14. Third Party Risk Management Policy and Procedures
15. Training Content related to CCPA (still under developed)
16. Sub-processor Llist