

## **Octagon Credit Investors, LLC – California Consumer Privacy Act of 2018 Privacy Notice and California Privacy Rights Act of 2020– (“California Privacy Notice”)**

### **Introduction – Octagon’s Commitment to You**

Octagon Credit Investors, LLC, together with its Broker Dealer affiliate Conning Investment Products, Inc. (all together “Octagon”) is committed to safeguarding the privacy and confidentiality of the Personal Information and Sensitive Personal Information you have entrusted us with. It is important for you to understand what Personal Information and Sensitive Personal Information Octagon will collect, how we will use it, and who may access it. The purpose of this notice is to provide you with information on our use of your Personal Information and Sensitive Personal Information in accordance with the California Consumer Privacy Act of 2018 (“CCPA”) and the California Privacy Rights Act of 2020 (“CPRA”).

### **Scope – Who does this California Privacy Notice apply to?**

The California Privacy Notice applies to the operations of Octagon in relation to California based consumers (i.e., natural persons and their households), including prospective and current investors in funds offered or managed by Octagon. Effective January 1, 2023, when the CPRA becomes operative, consumers covered under this California Privacy Notice will be expanded to include employees of companies doing business with Octagon (“B2B-related”) and Octagon employees and job applicants (as applicable). Please see our [Privacy Notice](#) for Octagon’s general operations with respect to consumers, including those outside of California.

Octagon’s websites may contain links to other third party websites. If you follow a link to any of those third party websites, please note that they have their own privacy policies and Octagon does not accept any responsibility or liability for their policies or processing of your Personal Information. Please check these policies before you submit any Personal Information to such third party websites.

### **What is Personal Information?**

Personal Information means information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular California resident - consumer or household. Personal Information excludes data made publicly available by the government. Personal Information includes, but is not limited to:

- a) Identifiers such as a real name, alias, postal address, telephone number, signature, unique personal identifier, online identifier, Internet Protocol address, email address, account name, social security number, driver’s license number, passport number, or other similar identifiers.
- b) Bank account number, credit card number, debit card number or any other financial information.
- c) Characteristics of protected classifications under California or federal law.
- d) Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.
- e) Biometric information, medical information, or health insurance information
- f) Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer’s interaction with an Internet Web site, application, or advertisement.
- g) Geolocation data.
- h) Audio, electronic, visual, thermal, olfactory, or similar information.
- i) Professional or employment-related information.

- j) Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 U.S.C. section 1232g, 34 C.F.R. Part 99).
- k) Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

### **What is Sensitive Personal Information (“SPI”)?**

Sensitive Personal Information means information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular California resident - consumer or household. Personal Information excludes data made publicly available by the government.

SPI includes, but is not limited to:

- a) Government ID — a consumer's Social Security, driver's license, state identification card, or passport number.
- b) Finances — a consumer's account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account.
- c) Geolocation — a consumer's precise geolocation.
- d) Race, religion and union membership — a consumer's racial or ethnic origin, religious or philosophical beliefs, or union membership.
- e) Communications — the contents of a consumer's private communications, unless the company is the intended recipient of the communication.
- f) Genetics — a consumer's genetic data.
- g) Biometrics — the processing of biometric information for the purpose of uniquely identifying a consumer.
- h) Health — personal information collected and analyzed concerning a consumer's health.
- i) Sexual orientation — personal information collected and analyzed concerning a consumer's sex life or sexual orientation.

### **Protecting Your Personal Information and Sensitive Personal Information**

Octagon has strict policies and procedures governing how it deals with your Personal Information and Sensitive Personal Information. Each and every one of Octagon's employees is responsible for respecting and protecting the Personal Information to which the employee has access.

Octagon's Compliance, Legal and Investor Relations departments in New York, USA oversee privacy governance including policy, consumer requests, dispute resolution, education, communications activities and reporting to Octagon's Board of Managers on privacy matters.

### **Personal Information and Sensitive Personal Information that Octagon Collects**

Octagon only collects the Personal Information or Sensitive Personal Information that the firm determines it needs for the purposes set out here.

To the extent Octagon collects, processes, or discloses Personal Information pursuant to the federal Gramm-Leach-Bliley Act (“GLBA”), such Personal Information, including consumer requests, is not subject to additional rights under the CCPA or CPRA, but is governed by Octagon's [Privacy Notice](#).

For example, Octagon may collect:

- **Information you provide to Octagon:** Personal Information or Sensitive Personal Information that you provide to Octagon, such as when using the contact form on Octagon’s websites, including your name, email address, and other contact details; employer information, issues of interest (to the extent that this amounts to Personal Information or Sensitive Personal Information) payment details and billing information;
- **Anti-Crime and Fraud Information:** Information which establishes your identity, such as government ID, or information about you from third parties, related to fraud, offenses, suspicious transactions, politically exposed person and sanctions lists where your details are included;
- **Financial Information, including financial needs and goals:** to ensure that the advice and/or products Octagon provides you are appropriate for you and the investments you purchase are suitable for you;
- **Your transactions and holdings:** details of transactions with Octagon or holdings with Octagon that you have made or initiated;
- **Our correspondence:** if you contact Octagon, we will typically keep a record of that correspondence;
- **Device Information:** such as information about your operating system, browser, software applications, IP address, geolocation, security status and other device information in order to improve your experience, to protect against fraud and manage risk;
- **Website and communication usage:** details of your visits to Octagon’s websites, client portals and information collected through cookies and other tracking technologies including, but not limited to, your IP address and domain name, your browser version and operating system, traffic data, location data, web logs and other communication data, and the resources that you access;
- **Marketing preference information:** details of your marketing preferences (e.g., communication preferences) and information relevant to selecting appropriate products and services to offer you;
- **Email tracking information:** Certain communications include links or metadata that allows Octagon to track opening of emails and clicks through to links within the email. Octagon may use this information for purposes including determining which of its emails or attachments are more interesting to you and to query whether users who do not open its emails or attachments wish to continue receiving them.
- **Survey information:** Octagon may also ask you to complete surveys that Octagon uses for research purposes. In such circumstances Octagon shall collect the information provided in the completed survey.

## **Purposes for which we use your Personal Information or Sensitive Personal Information**

When Octagon collects your Personal Information or Sensitive Personal Information, Octagon may use or disclose it for the following purposes:

- **To provide and manage products and services you have requested** ► to administer Octagon’s services, including to carry out its obligations arising from any agreements entered into between you and Octagon, or to notify you about changes to Octagon’s services and products.
- **To verify your identity, protect against fraud and manage risk** ► Octagon and other organizations may access and use certain information to prevent fraud, money laundering and terrorism as may be required by applicable law and regulation and best practice at any given time, including checking against sanctions, politically exposed persons (PEP) and other fraud or crime screening databases. If false or inaccurate information is provided and fraud is identified or suspected, details may be passed to fraud prevention agencies and may be recorded by Octagon or by them.
- **To comply with legal or regulatory requirements, or as otherwise permitted by law** ► Octagon may process your Personal Information or Sensitive Personal Information to comply with its regulatory requirements or dialogue with its regulators or defend or prosecute claims as applicable which may include disclosing your Personal Information or Sensitive Personal Information to third parties, the court service and/or regulators or law enforcement agencies in connection with enquiries, proceedings or investigations by such parties anywhere in the world. Where permitted, Octagon will direct any such request to you or notify you before responding unless to do so would prejudice the prevention or detection of a crime.
- **To monitor certain activities** ► to monitor queries and transactions to ensure service quality, compliance with procedures and to combat fraud.
- **To inform you of changes** ► to notify you about changes to Octagon’s services and products.
- **To communicate with you regarding products and services that may be of interest** ► to provide you with updates and offers, where you have chosen to receive these. Octagon may also use your information for marketing Octagon’s own products and services to you by post, email, phone or online or social media advertisement. Where required by law, Octagon will ask for your consent at the time Octagon collects your data to conduct any of these types of marketing.
- **To understand Octagon’s customers and to develop and tailor Octagon’s products and services** ► Octagon may analyze the Personal Information it holds in order to better understand Octagon’s clients’ services and marketing requirements, to better understand Octagon’s business and develop Octagon’s products and services. In order to ensure that content from Octagon’s website is presented in the most effective manner for you and for your device, Octagon may pass your data to business partners, suppliers and/or service providers.
- **To reorganize or make changes to Octagon’s business** ► in the event that Octagon (i) is subject to negotiations for the sale of Octagon’s business or part thereof to a third party, (ii) are sold to a third party or (iii) undergo a reorganization, Octagon may need to transfer some or all of

your Personal Information to the relevant third party (or its advisors) as part of any due diligence process for the purpose of analyzing any proposed sale or reorganization. Octagon may also need to transfer your Personal Information to that reorganized entity or third party after the sale or reorganization for them to use for the same purposes as set out in this policy.

- **To communicate effectively with you and conduct Octagon’s business** ► to conduct Octagon’s business, including to respond to your queries, to otherwise communicate with you, or to carry out its obligations arising from any agreements entered into between you and Octagon.

### **Consumer Rights under CCPA and CPRA**

California consumers have certain rights under CCPA and CPRA. Please note that a consumer’s exercise of these rights is subject to certain exemptions to safeguard the public interest (e.g., the prevention or detection of crime) and Octagon’s interests (e.g., the maintenance of legal privilege). For rights exercised by consumers, Octagon will disclose and deliver the required information to a consumer free of charge within 45 days of receiving a verifiable request after Octagon has verified that the person requesting the information is the consumer or authorized persons permitted to receive such information.

With respect to Personal Information or Sensitive Personal Information that Octagon collects, processes, or discloses pursuant to the GLBA, only the *Private Right of Action* will be applicable.

- **Right to Know/Notice** – Consumers shall have the right to know what Personal Information or Sensitive Personal Information is collected, used, shared or sold, both as to the categories and specific pieces of Personal Information or Sensitive Personal Information.
- **Right to Access/Portability** – Consumers have the right to request that a business disclose the *categories* of Personal Information and Sensitive Personal Information collected; the categories of *sources* from which Personal Information or Sensitive Personal Information is collected; the *business or commercial purpose*; the categories of *third parties* with which the business discloses Personal Information or Sensitive Personal Information; and the *specific pieces* of Personal Information or Sensitive Personal Information the business holds about a consumer. *Under the CCPA, Octagon shall not be required to provide Personal Information to a consumer more than twice in a 12-month period.*
- **Right to Erasure** – Consumers shall have the right to request that a business delete any Personal Information about the consumer which the business has collected from the Consumer. *Under the CPRA, Octagon will notify and instruct service providers, contractors, or other third parties who have received a consumer’s Personal Information or Sensitive Personal Information and request deletion, as appropriate, when in receipt of a Verifiable Consumer Request.*
- **Right to Equal Service** – Consumers shall have the right to non-discrimination in terms of price or service when a consumer exercises a privacy right under CCPA and CPRA.
- **The Right to Opt Out** – Consumers shall have the right to opt-out of sale or Sharing of Personal Information and Sensitive Personal Information. *Please note that Octagon does not sell or Share, as defined under the CPRA, Personal Information to third party service providers. The CPRA expands the CCPA’s “Do Not Sell” opt-out requirements to mere “sharing” of personal information for purposes of cross-context behavioral advertising (i.e., interest-based advertising*

*or retargeting, specifically, the targeting of advertising to a consumer based on personal information from the consumer's interactions with other business, websites, etc.)*

- **Private Right of Action** – The CCPA creates a new private right of action with statutory damages for consumers whose nonencrypted and nonredacted Personal Information is subject to an unauthorized access and exfiltration, theft or disclosure as a result of a business's violation of the duty to implement and maintain reasonable security procedures and practices. *The CPRA expands the Private Right of Action by creating a new category of data, Sensitive Personal Information, for which a private cause of action may be brought.*

The CPRA creates two additional rights for California consumers:

- **Right to Correct** – Consumers shall have the right to correct inaccurate Personal Information or Sensitive Personal Information. *A consumer shall have the right to submit a request to correct information if Octagon maintains inaccurate Personal Information or Sensitive Personal Information, taking into account the nature of the Personal Information or Sensitive Personal Information and the purpose of the processing of such information.*
- **Right to Limit Use and Disclosure** – Consumers have the right to limit the use and disclosure of Sensitive Personal Information (“SPI”). *If Octagon uses or discloses SPI for purposes other than those stated as those necessary to perform the services reasonably expected by the consumer, Octagon must notify the Consumer and provide them with the right to limit its use and/or disclosure.*

For the avoidance of doubt, the obligations imposed on Octagon by CCPA and CPRA shall not restrict our obligation to 1) comply with federal, state, or local laws; 2) comply with civil criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state or local authorities; 3) cooperate with law enforcement agencies concerning conduct or activity that Octagon, service providers, or third parties reasonably and in good faith believes may violate federal state or local law; 4) exercise or defend legal claims; or 5) collect, use, retain, or disclose consumer information that is deidentified or in the aggregate consumer information.

### **Disclosing your Personal Information or Sensitive Personal Information**

Octagon will only use or disclose your Personal Information or Sensitive Personal Information for the purpose(s) it was collected and as otherwise identified in this California Privacy Policy. As noted, Octagon will not sell Personal Information or Sensitive Personal Information. Additionally, as defined under the CPRA, Octagon does not currently and does not intend to “Share” i.e., disclose, make available, transfer, or communicate a consumer's Personal Information or Sensitive Personal Information to a third party for “cross-context behavioral advertising”, whether or not for monetary or other valuable consideration.

**Disclosing outside Octagon:** Personal Information or Sensitive Personal Information may be provided to third parties or service providers, including anti-fraud organizations, legal, regulatory or law enforcement authorities in cases of suspected criminal activity or contravention of law, for the detection and prevention of fraud, or when required to satisfy the legal or regulatory requirements of governments, regulatory authorities or other self-regulatory organizations, or to comply with a court order or for the protection of Octagon's assets (for example, collection of overdue accounts).

**Disclosing with Octagon affiliates:** Octagon may disclose your Personal Information or Sensitive Personal Information with affiliates for legal and regulatory purposes, to manage credit risk and other business risks, to perform analytics, to ensure Octagon has correct or up to date information about you (such as your current address or date of birth) and to better manage your relationship with Octagon.

**Business sale or reorganization:** Over time, Octagon may buy new businesses or sell some of its businesses. Accordingly, Personal Information associated with any accounts, products or services of the business being purchased or sold will be reviewed as part of the due diligence process and subsequently transferred as a business asset to the new business owner. Octagon may also transfer Personal Information or Sensitive Personal Information as part of a corporate reorganization or other change in corporate control.

**Sub-contractors and agents:** Octagon may use affiliates or other companies to provide services on its behalf such as data processing, account administration, fraud prevention and detection, analytics and marketing. Such companies will be given only the Personal Information or Sensitive Personal Information needed to perform those services and Octagon does not authorize them to use or disclose Personal Information or Sensitive Personal Information for their own marketing or other purposes. Octagon has contracts in place holding these companies to the same standards of confidentiality by which Octagon is governed.

### **Safeguarding your Personal Information and Sensitive Personal Information**

Octagon uses physical, electronic and procedural safeguards to protect against unauthorized use, access, modification, destruction, disclosure, loss or theft of your Personal Information and Sensitive Personal Information in Octagon's custody or control.

Octagon has agreements and controls in place with third party service providers requiring that any information Octagon provides to them must be safeguarded and used only for the purpose of providing the service Octagon has requested the company to perform.

In order to safeguard Personal Information and Sensitive Personal Information, upon receiving a Verifiable Consumer Request ("VCR"), Octagon will authenticate the VCR and validate that the person requesting the information is the consumer or authorized persons permitted to receive such information.

#### *Security over the internet*

No data transmission over the Internet or website can be guaranteed to be secure from intrusion. However, Octagon maintains commercially reasonable physical, electronic and procedural safeguards to protect your Personal Information in accordance with data protection legislative requirements.

All information you provide to Octagon is stored on its or Octagon's subcontractors' secure servers and accessed and used subject to Octagon's security policies and standards. Where Octagon has given you (or where you have chosen) a password which enables you to access certain parts of Octagon's websites, you are responsible for keeping this password confidential and for complying with any other security procedures of which you have been notified by Octagon. Octagon asks you not to share a password with anyone.

### **Changes to this California Privacy Notice**

From time to time, Octagon may make changes to this California Privacy Notice.

This California Privacy Notice at <https://www.octagoncredit.com> is always the most recent version.

## **Contact Us**

Should you have any queries or wish to discuss your data protection rights with us, please contact us by calling the toll-free number 888-266-6464 and following the menu instructions to reach any of the Octagon personnel listed below or by contacting Octagon directly at 212-400-8400.

Erin Crawford, Head of Investor Relations  
[investorrelations@octagoncredit.com](mailto:investorrelations@octagoncredit.com)

Margaret Julian, Chief Compliance Officer  
[mjulian@octagoncredit.com](mailto:mjulian@octagoncredit.com)

Geoffrey Dorment, General Counsel  
[gdorment@octagoncredit.com](mailto:gdorment@octagoncredit.com)

Octagon Credit Investors, LLC  
Investor Relations  
250 Park Avenue, 15th Floor, New York, NY 10177

**Notice updated as of:** January 2023