Consumer Privacy Policy

Purpose

Class Valuation, LLC and its subsidiaries and affiliates (hereinafter collectively referred to as the "Company") provide appraisal services to institutional lenders and real estate firms throughout the United States. Due to the nature of those services, the Company regularly obtains personal information about consumers that must be kept private and secure from third parties who could use it to commit identify theft or other crimes. In addition to client requirements that such information be kept confidential to prevent fraud, the Company is subject to privacy laws designed to ensure that personal and sensitive information about consumers who receive loans or related products from financial service providers not be sold or used in ways that the consumer did not anticipate or approve. Failure to comply with privacy laws can result in monetary fines, costly litigation, and other penalties. Therefore, the Company has implemented this Consumer Privacy Policy to ensure compliance with applicable privacy statutes and mitigate the risks associated with the unauthorized disclosure of sensitive consumer information.

This policy identifies applicable consumer privacy laws and outlines the steps necessary for compliance. All Company employees and third-party service providers who perform services on behalf of the Company are required to adhere to this policy, following procedural safeguards, and always maintain the confidential nature of sensitive consumer information.

Approval and Administration

The Company's Legal and Compliance Department is responsible for the oversight, development, implementation, and administration (including staff training and oversight of third-party service providers) of this policy and shall approve all policy updates.

Consumer Privacy Laws Applicable to the Company

A. Gramm Leach-Bliley Act (GLBA)

The Gramm Leach-Bliley Act (also known as the Financial Modernization Act of 1999) is a federal law enacted to control the way financial institutions deal with the private information of individuals. In order to be GLBA compliant, financial institutions must inform consumers how their sensitive data is used, inform them of their right to opt-out if they prefer that their personal data not be shared with third parties, and apply specific protections to consumers' private data in accordance with a written information security plan created by the institution.

The GLBA consists of three sections:

1. The **Financial Privacy Rule**, which regulates the collection and disclosure of private financial information.
2. The **Safeguards Rule**, which stipulates that financial institutions must implement security programs to protect such information.
3. The **Pretexting provisions**, which prohibit the practice of pretexting, *i.e.*, presenting oneself as someone else in order to obtain private information about another person.

The GLBA requires that financial institutions act to ensure the confidentiality and security of consumers' "nonpublic personal information" (commonly referred to as "NPI"). NPI includes Social Security numbers, credit and income histories, credit and bank card account numbers, telephone numbers, addresses, names, and any other personal information received by a financial institution that is to be kept private. The Safeguards Rule states that financial institutions must create a written information security plan describing the program to protect their customers' information. The information security plan must be tailored specifically to the institution's size, operations, and complexity, as well as the sensitivity of the customers' information. According to the Safeguards Rule, covered financial institutions must:

- Designate one or more employees to coordinate its information security program.
- Identify risks to consumer information in each aspect of the company's operation and evaluate the effectiveness of existing safeguards for controlling those risks.
- Design and implement a safeguard program and regularly monitor and test it.
- Select third party service providers that can maintain appropriate safeguards for consumer data, ensure that service contracts require third party vendors to maintain adequate safeguards, and oversee the handling of consumer information; and
- Evaluate and adjust the program in light of relevant circumstances, including changes in the company's business or operations, or the results of security testing and monitoring.

In order to achieve GLBA compliance, the Safeguards Rule requires that financial institutions pay special attention to employee management and training, information systems, and security management in their information security plans and implementation. The Company meets these objectives by (1) training employees to follow procedures designed to maintain the confidentiality of NPI; (2) utilizing third-party service providers who must pass a criminal background check and execute service contracts requiring them to implement data security measures to protect NPI; and (3) adhering to the Company's written Information Security Policy, which is administered by several employees charged with safeguarding sensitive data and which contains comprehensive rules regarding computer usage, building security, computer systems security, data security, records management, data disposal and data encryption.

B. State Specific Privacy Laws

Introduction:

Some of the Personal Data the Company collects constitutes "personal information" or "sensitive personal information" under the California Consumer Privacy Act of 2018 ("CCPA") and the California Privacy Rights Act of 2020 ("CPRA") or "personal data" or "sensitive data" under the Virginia Consumer Data Protection Act ("VCDPA"), the Colorado Privacy Act ("ColoPA"), the Connecticut Act Concerning Personal Data Privacy and Online Monitoring ("CTDPA"), Utah Consumer Privacy Act ("UCPA"), or other similar state laws. Any such "sensitive personal information" or "sensitive data" is referred to as "Sensitive Data" herein.

Categories of Information Collected:

The Company collects various Personal Data Categories including, but not limited to, identifiers, California Customer Records personal information, protected classification characteristics under state or federal law, commercial information, geolocation data and sensory data.

Examples of the personal data or personal information in each of the categories above are:

- **Identifiers:** A real name, alias, postal address, 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.
- **California Custodial Records personal information:** A name, signature, Social Security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information.
- **Protected classification characteristics under state or federal law:** Age (40 years or older), citizenship, marital status, medical condition, physical or mental disability, sex (including gender, gender identity, gender expression, pregnancy or childbirth and related medical conditions), veteran or military status.
- **Commercial Information:** Records of personal property to the extent necessary for Uniform Commercial Code security interest filings
- **Geolocation data:** Physical location Does not include precise geolocation, which is Sensitive Data.
- **Sensory data:** Audio, electronic, visual, thermal, olfactory, or similar information as necessary for accommodating the needs of the individual.
- **Government Identifiers:** Social security, driver's license, state identification card or passport number
- **Precise geolocation:** Not applicable to the Company

Sources of Personal Data collected:

The Company obtains the categories of Personal Data listed above from the following categories of sources:

- Directly from the consumer. For example, from forms the consumer completes or products and services the consumer purchases.
- Indirectly from the consumer. For example, from observing actions on the Website.
- From the Company's affiliates and subsidiaries. From third party sources, including information from commercially available sources, such as public databases and data aggregators.
- From the financial services clients that request services from the Company. The Company may disclose consumer Personal Data or Sensitive Data to a third party for a business purpose. When the Company discloses Personal Data or Sensitive Data for a business purpose, the Company enters into a contract that describes the purpose and requires the recipient to both keep that Personal Data and Sensitive Data confidential and not use it for any purpose except performing the contract. The Company discloses this Personal Data and Sensitive Data for a business purpose to the following categories of third parties:
    - consumer relations, including consumer complaint response services.
    - employee recruitment, career portal and job applicant services.

Consumer Rights:

As applicable, certain state privacy laws, such as the CCPA, CPRA, ColoPA, VCDPA, CTDPA, and UCPA provide their residents, respectively, with specific rights regarding their Personal Data.

a. ***Access to Specific Information and Data Portability Rights.*** The consumer has the right to request that the Company disclose certain information to the consumer about the Company's collection and use of the consumer's Personal Data and Sensitive Data. Once the Company receives and verifies the request (See Subsection ***Exercising Access, Data Portability, Correction, and Deletion Rights*** below for more information), the Company will disclose to the consumer, as applicable:
    - The categories of Personal Data and Sensitive Data the Company collected about the consumer.
    - The categories of sources for the Personal Data and Sensitive Data the Company collected about consumer.
    - The Company's business or commercial purpose for collecting that Personal Data and Sensitive Data.
    - The categories of third parties with whom the Company disclosed that Personal Data and Sensitive Data.
    - The specific pieces of Personal Data and Sensitive Data the Company collected about the consumer (also called a data portability request).

b. ***Correct Specific Information.*** The consumer may have the right to request that the Company corrects inaccurate Personal Data about the consumer. Once the Company receives and verifies the request (see Subsection ***Exercising Access, Data Portability, Correction, and Deletion Rights*** below for more information), the Company will use commercially reasonable efforts to correct the information to comply with the request. This right is not afforded to residents of Utah.

c. ***Deletion Request Rights***. The consumer has the right to request that the Company delete any of the consumer's Personal Data or Sensitive Data that was collected from the consumer and retained, subject to certain exceptions. Once the Company receives and verifies the request (see Subsection ***Exercising Access, Data Portability, Correction, and Deletion Rights*** below for more information), the Company will delete (and direct its service providers to delete) the Personal Data or Sensitive Data from the Company's records, unless an exception applies. In responding to the consumer request, the Company will inform the consumer whether or not the Company has complied with the request, and, if the Company has not complied, provide the consumer with an explanation as to why.

A service provider shall not be required to comply with a deletion request submitted by the consumer directly to the service provider.

The Company may deny a consumer deletion request if retaining the information is necessary for the Company, or a service provider(s), to:

- Complete the transaction for which the Company collected the Personal Data, provide a good or service that the consumer requested, take actions reasonably anticipated within the context of the Company's ongoing business relationship with the consumer, or otherwise perform the Company's contract with the consumer.
- Help to ensure security and integrity to the extent the use of the consumer's Personal Data is reasonably necessary and proportionate for those purposes.
- Debug products to identify and repair errors that impair existing intended functionality.
- Exercise free speech, ensure the right of another consumer to exercise his/her free speech rights, or exercise another right provided for by law.
- Comply with the California Electronic Communications Privacy Act (Cal. Penal Code § 1546 et. seq.).
- Engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws, when the information's deletion may likely render impossible or seriously impair the research's achievement, if the consumer previously provided informed consent.
- Enable solely internal uses that are reasonably aligned with consumer expectations based on the consumer's relationship with us.
- Comply with a legal obligation.

d. ***Right to Limit Use and Disclosure of Sensitive Data.*** The consumer may have the right, at any time, to direct the Company to limit its use and disclosure of the consumer's Sensitive Data to use which is necessary for certain purposes enumerated in applicable law ("Enumerated Purposes"). To the extent the Company uses or discloses the consumer's Sensitive Data for purposes other than the Enumerated Purposes (described below), the consumer has the right to limit such use or disclosure. Currently, the Company does not use Sensitive Data for purposes other than the Enumerated Purposes. To the extent applicable, the consumer may also have the right to withdraw consent the consumer provided for the Company's use and disclosure of the consumer's Sensitive Data.

The Enumerated Purposes include the following:

(1) To perform the services or provide the goods reasonably expected by an average consumer who requests those goods or services.

(2) To detect security incidents that compromise the availability, authenticity, integrity, and confidentiality of stored or transmitted Personal Data, including Sensitive Data.

(3) To resist malicious, deceptive, fraudulent, or illegal actions directed at the Company 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, non-personalized advertising shown as part of a consumer's current interaction with the Company, provided that the Company will not disclose the Sensitive Personal Data, to another third party and will not use it to build a profile about the consumer or otherwise alter the consumer's experience outside the current interaction with the Company.

(6) To perform services on behalf of the Company, such as maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing financing, providing analytic services, providing storage, or providing similar services on behalf of the Company's business.

(7) To verify or maintain the quality or safety of a service or device that is owned, manufactured, manufactured for, or controlled by the Company, and to improve, upgrade, or enhance the service or device that is owned, manufactured by, manufactured for, or controlled by the Company.

Role of Class Valuation, LLC:

Due to the volume of business the Company performs in California in addition to the other states included above, the Company is subject to the terms under the California Consumer Privacy Act of 2018 ("CCPA") and the California Privacy Rights Act of 2020 ("CPRA"), the Virginia Consumer Data Protection Act ("VCDPA"), the Colorado Privacy Act ("ColoPA"), the Connecticut Act Concerning Personal Data Privacy and Online Monitoring ("CTDPA"), Utah Consumer Privacy Act ("UCPA"), or other similar state laws. The Company must therefore ensure that the Company and all third-party service providers performing services on its behalf use personal information in a manner that complies with all applicable laws. This means that neither the Company nor any of its vendors may retain, use, or disclose consumer personal information for any purpose other than the sole and specific purpose of performing the service ordered by the consumer, or as otherwise permitted. In addition, the Company implemented the following measures to become compliant:

- The Company updated the Privacy Policy displayed on its website to explain how it uses data provided by consumers.
- The Company created a telephone hotline for consumers who wish to inquire about the use of their personal information; and
- The Company created a website portal that allows California and Virginia consumers to submit written requests for information about the use and handling of their personal information in connection with the services provided by the Company.
- The Company includes the Privacy Policy in all closing packages provided to consumers.
- The Company, through the Compliance Department, will respond to verified consumer requests in a timely manner and in accordance with state law.

Role of Third-Party Vendors:

Third-party vendors who provide services to consumers on behalf of the Company are contractually required to comply with the applicable privacy laws as well. Specifically, vendors who provide services for the Company are now expressly required to:

- delete any personal information that they obtained from the Company, unless permitted by law to retain such information.
- warrant that they do not and will not sell personal information provided or made available to them by the Company; and
- refrain from sharing any personal information with other business entities or subcontractors unless the Company authorizes such disclosure, and the disclosure is necessary to perform a service ordered by the Company.

Monitoring Pending Legislation

As of January 2023, five states have signed privacy laws that go into effective in 2023 and four have active pending bills. The Company will actively monitor these bills to ensure compliance if and when they become law. In addition, there is proposed federal law, the American Data Privacy and Protection Act (ADPPA), that the Company will continue to track.

Updates and Annual Review Process

This Consumer Privacy Policy will be reviewed and updated at least annually by the Company's Legal and Compliance Departments. In addition, the Company will update this policy whenever a new consumer privacy law goes into effect or lawmakers promulgate new guidelines with respect to existing law.

Revision History

The table below provides an audit trail of the changes made to this document. All changes to the policy must be documented in this table as well as reviewed and approved by the VP of Compliance and/or the Chief Legal Officer.

Date	Version	Approved by	Changes by	Summary of Changes
03/28/2025	1.0	Blair Dingeman	Blair Dingeman	Original policy