FOR MORE INFORMATION

GENTRY LOCKE
Roanoke, VA
www.gentrylocke.com

Paul G. Klockenbrink
klockenbrink@gentrylocke.com

Virginia

Are mandatory arbitration provisions recognized in your state? If so, are there any limitations to its enforcement?

Mandatory arbitration provisions are generally enforceable in Virginia pursuant to Va. Code Ann. § 8.01-581.01. Therefore, agreements to submit existing or future controversies to arbitration are considered "valid, enforceable, and irrevocable," provided they are in writing and otherwise contractually valid. When such an agreement is ignored and a proceeding is commenced, a court must order the parties to arbitrate upon application and a showing of a valid mandatory arbitration agreement by one party. Va. Code Ann. § 8.01-581.02. Likewise, a party may apply for a stay of proceedings in violation of a valid mandatory arbitration agreement. Id.

While these agreements are generally enforceable, they have been held unenforceable in certain situations. First, pursuant to a recent Supreme Court of Virginia decision, mandatory arbitration provisions in trusts are unenforceable against beneficiaries. Boyle v. Anderson, 871 S.E.2d 226, 2022 Va. Lexis 22 (2022). Second, in 2019, the Virginia State Corporation Commission issued a regulation which prohibits investment advisers operating in Virginia from including mandatory arbitration provisions in advisory contracts. 21-VAC5-80-200(F). However, this rule is likely preempted by the Federal Arbitration Act and, therefore, unenforceable if challenged in federal court.

What is your state's law, if any, regarding gift cards, subscription services and loyalty programs?

GIFT CARDS

- 55.1-2515. Gift certificates and credit balances.
    - Except as described in subsection B, a gift certificate or credit balance issued in the ordinary course of the issuer's business that has remained unclaimed by the owner for more than five years after such gift certificate or credit balance became payable is presumed abandoned.
    - The following property is exempt from the provisions of this chapter and shall not be assessed by the administrator as unclaimed property:
        - credit balances payable to a business association;
        - outstanding checks resulting from or attributable to the sale of goods or services to a business association;
        - promotional incentives; and
        - credits, gift certificates, coupons, layaways, and similar items, provided that such credits, gift certificates, coupons, layaways, and similar items are redeemable in merchandise, in services, or through future purchases.

- § 59.1-530. Definitions.
- As used in this chapter, unless the context clearly requires otherwise:
- "Gift certificate" or "certificate" means a certificate, electronic card, or other medium issued by a merchant that evidences the giving of consideration in exchange for the right to redeem the certificate, electronic card, or other medium for goods, food, services, credit, or money of at least an equal value, including any electronic card issued by a merchant with a banked dollar value where the issuer has received payment for the full banked dollar value for the future purchase, or delivery, of goods or services and any certificate issued by a merchant where the issuer has received payment for the full face value of the certificate for future purchases, or delivery, of goods or services.
- "Merchant" means an owner or operator of any mercantile establishment or any agent, employee, lessee, consignee, officer, director, franchisee, or independent contractor of such owner or operator.
- § 59.1-531. Required disclosures.
    - Each gift certificate issued by a merchant in the Commonwealth that has an expiration date shall include either (i) a statement of the expiration date of the certificate or (ii) a telephone number or Internet address where the holder of the certificate may obtain information regarding the expiration date of the certificate.
    - Each gift certificate issued by a merchant in the Commonwealth that diminishes in value over time shall include a telephone number or Internet address where the holder of the certificate may obtain information regarding the diminution in the value of the certificate over time.
    - The information required by this section shall be clearly and permanently imprinted on the certificate.
- § 59.1-532. Enforcement; penalties.
    - Any violation of the provisions of this chapter shall constitute a prohibited practice pursuant to the provisions of § 59.1-200 and shall be subject to any and all of the enforcement provisions of Chapter 17 (§ 59.1-196 et seq.) of this title.

SUBSCRIPTION SERVICES

- § 59.1-207.45. Definitions.
    - As used in this chapter, unless the context requires a different meaning:
        - "Automatic renewal" means a plan or arrangement in which a paid subscription or purchasing agreement is automatically renewed at the end of a definite term for a subsequent term of more than one month.
        - "Automatic renewal offer terms" means the following clear and conspicuous disclosures:
            - That the subscription or purchasing agreement will continue until the consumer cancels;
            - The description of the cancellation policy that applies to the offer;

- The recurring charges that will be charged to the consumer's credit or debit card or payment account with a third party as part of the automatic renewal plan or arrangement and that the amount of the charge may change, if that is the case, and the amount to which the charge will change, if known;
- The length of the automatic renewal term or that the service is continuous, unless the length of the term is chosen by the consumer; and
- The minimum purchase obligation, if any.

- "Clear and conspicuous" or "clearly and conspicuously" means in larger type than the surrounding text, or in contrasting type, font, or color to the surrounding text of the same size, or set off from the surrounding text of the same size by symbols or other marks, in a manner that clearly calls attention to the language. In the case of an audio disclosure, "clear and conspicuous" or "clearly and conspicuously" means in a volume and cadence sufficient to be readily audible and understandable.
- "Consumer" means any individual who seeks or acquires, by purchase or lease, any goods, services, money, or credit for personal, family, or household purposes.
- "Continuous service" means a plan or arrangement in which a subscription or purchasing agreement continues until the consumer cancels the service.
- "Supplier" has the same meaning ascribed thereto in § 59.1-198.

- § 59.1-207.46. Making automatic renewal or continuous service offer to consumer; affirmative consent required; disclosures; prohibited conduct.
  - No supplier making an automatic renewal or continuous service offer to a consumer in the Commonwealth shall do any of the following:
    - Fail to present the automatic renewal offer terms or continuous service offer terms in a clear and conspicuous manner before the consumer becomes obligated on the automatic renewal or continuous service offer and in visual proximity, or in the case of an offer conveyed by voice, in temporal proximity, to the request for consent to the offer.
    - Charge the consumer's credit or debit card or the consumer's account with a third party for an automatic renewal or continuous service without first obtaining the consumer's affirmative consent to the agreement containing the automatic renewal offer terms or continuous service offer terms.
    - Fail to provide an acknowledgment that includes the automatic renewal or continuous service offer terms, cancellation policy, and information regarding how to cancel in a manner that is capable of being retained by the consumer. If the offer includes a free trial, the supplier shall also disclose in the acknowledgment how to cancel the free trial before the consumer pays or becomes obligated to pay for the goods or services.

- A supplier making automatic renewal or continuous service offers shall provide a toll-free telephone number, an electronic mail address, a postal address only when the supplier directly bills the consumer, or another cost-effective, timely, and easy-to-use mechanism for cancellation that shall be described in the acknowledgment specified in subdivision A 3. Each supplier making automatic renewal or continuous service offers through an online website shall make available a conspicuous online option to cancel a recurring purchase of a good or service.
- In the case of a material change in the terms of the automatic renewal or continuous service offer that has been accepted by a consumer in the Commonwealth, the supplier shall provide the consumer with a clear and conspicuous notice of the material change and provide information regarding how to cancel in a manner that is capable of being retained by the consumer.
- A supplier making automatic renewal or continuous service offers that include a free trial lasting more than 30 days shall, within 30 days of the end of any such free trial, notify the consumer of his option to cancel the free trial before the end of the trial period to avoid an obligation to pay for the goods or services.
- The requirements of this section shall apply only prior to the completion of the initial order for the automatic renewal or continuous service, except:
  - The requirement in subdivision A 3 may be fulfilled after completion of the initial order; and
  - The requirement in subsection C shall be fulfilled prior to implementation of the material change.

- § 59.1-207.47. When goods, wares, merchandise, or products deemed a gift.
  - In any case in which a supplier sends any goods, wares, merchandise, or products to a consumer under a continuous service agreement or automatic renewal of a purchase without first obtaining the consumer's affirmative consent as described in § 59.1-207.46, the goods, wares, merchandise, or products shall for all purposes be deemed an unconditional gift to the consumer, who may use or dispose of the same in any manner he sees fit without any obligation whatsoever on the consumer's part to the supplier, including any obligation or responsibility for shipping any goods, wares, merchandise, or products to the supplier.
- § 59.1-207.48. Exemptions.
  - This chapter shall not apply to:
  - Any service provided by a supplier or its affiliate where either the supplier or its affiliate is doing business pursuant to a franchise issued by a political subdivision of the Commonwealth or a license, franchise, certificate, or other authorization issued by the State Corporation Commission to a public service company or public utility pursuant to Title 56;

- Any service provided by a supplier or its affiliate where either the supplier or its affiliate is regulated by the State Corporation Commission, the Federal Communications Commission, or the Federal Energy Regulatory Commission;
- Alarm company operators that are regulated pursuant to § 15.2-911;
- A bank, bank holding company, or the subsidiary or affiliate of either, or a credit union or other financial institution, licensed under federal or state law;
- Any home protection company regulated by the State Corporation Commission pursuant to Chapter 26 (§ 38.2-2600 et seq.) of Title 38.2;
- Any home service contract provider regulated by the Department of Agriculture and Consumer Services pursuant to Chapter 33.1 (§ 59.1-435 et seq.);
- Any insurer or entity regulated under Title 38.2 or an affiliate of such insurer or entity; or
- Any health club registered pursuant to the Virginia Health Club Act (59.1-294 et seq.).

- § 59.1-207.49. Enforcement; penalties.
  - Any violation of this chapter shall constitute a prohibited practice under the provisions of § 59.1-200 and shall be subject to the enforcement provisions of the Virginia Consumer Protection Act (§ 59.1-196 et seq.). However, if a supplier makes a good faith effort to comply with the requirements of this chapter, the supplier shall not be subject to either a civil penalty under § 59.1-206 or damages under § 59.1-204.

LOYALTY PROGRAMS

There are no applicable laws, however, Va. Code § 59.1-578 may have some application as to the collection of data.

What is your state's law, if any, regarding safeguarding consumer credit card or other private data (i.e., cyber security)? / What is your state's law, if any, regarding the collection and handling of financial information?

The Virginia Consumer Data Privacy Act ("VCDPA") is Virginia's law protecting consumer data, including credit information, financial information, and other forms of personal information. [i]

Fortunately, Virginia's law is seen as one of the most business-friendly of the data privacy laws. Most importantly, the VCDPA (i) does not provide a private right of action, but rather vests enforcement responsibility with the state Attorney General, and (ii) it affords controllers and processors a 30-day cure period following notice of an alleged violation before the Attorney General may initiate an enforcement action.

GENERAL VCDPA REQUIREMENTS

The following are the most important requirements imposed by the VCDPA.

- Data Minimization - Collect only what is adequate, relevant, and reasonably necessary.
- Transparency/Notice – Provide consumers with a reasonably accessible, clear, and meaningful privacy notice that includes data use and disclosure practices and targeted advertising and opt-out disclosures.

- Security Safeguards – Implement data security practices that adequately protect personal information.
- Privacy-by-design (Assessments) – Conduct data protection assessments when required.
- Vendor Contracts – Maintain a contract to establish data processing procedures with third-parties processing data on behalf of the organization
- Appeals – Implement an internal appeal process for consumers who appeal the organization's denial of a data request.

SCOPE – MUST YOUR COMPANY COMPLY WITH THE VCDPA?

The most important consideration for any company faced with a new privacy law, is whether that law even applies to them. The VCDPA uses specific numerical thresholds for determining applicability.

The VCDPA applies to organizations that do business in the Commonwealth of Virginia or organizations that produce products or services that are targeted to residents of Virginia. In addition, these organizations must also meet one of the following criteria:

- Process or control the personal data of at least 100,000 consumers in a calendar year;

OR

- Process or control the personal data of at least 25,000 consumers and derive over 50% of gross revenue from selling that data

The definitions of the terms contained within the VCDPA, as well as the many exemptions written into the law, flesh out the full scope of this privacy framework.

- Definitions

The definitions of "personal data" and "consumer" are key to understanding whether your company falls within the scope of the VCDPA.

Personal Data – The VCDPA defines personal data as "any information that is linked or reasonably linkable to an identified or identifiable natural person."

  - This definition is broad in that it includes "any information," but is narrowed by the fact that the information must be traceable to a "natural person" (not an organizational entity).
  - The law does not outline specific examples of personal data, however, it does provide for certain exemptions that are critical to understanding the scope of the VCDPA (below).

Consumer – A "consumer" is any Virginia resident, but only to the extent of his or her activity in an individual or household context. When acting as an employee or as a representative of an organization, an individual is not a "consumer" for VCDPA purposes.

  - Processing the personal data of a company's own employees, or gathering personal data on officers of other companies, is not relevant for purposes of calculating the number of "consumers" whose personal data is being processed.

Process – As used in the VCDPA, "processing data" is a broad term that encompasses any operation performed on data, including collection, use, storage, disclosure, analysis, deletion, or modification of the data.

- Exemptions

There are several exemptions that can be found under the VCDPA, including organizational exemptions, exemptions to covered information, and specific exemptions for certain data types.

The organizational exemptions apply to organizations including:

  - State government agencies
  - Financial institutions subject to Gramm-Leach-Bliley Act (GLBA)
  - Covered entities and business associates under the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH)
  - Non-profit organizations
  - Higher education institutions

There are also exemptions for information covered under sectoral laws including:

  - Children's Online Privacy Protection Act (COPPA)
  - Drivers Privacy Protection Act
  - Fair Credit Reporting Act (FCRA)
  - Family Educational Rights and Privacy Act (FERPA)
  - Farm Credit Act
  - GLBA
  - HIPAA
  - HITECH

Finally, the VCDPA provides exemptions for certain types of personal information. These include:

- De-identified personal data – data that cannot be linked to a natural person. Personal data can be de-identified or anonymized to remove the data from the ambit of the VCDPA.
- Publicly available information – information made available through government records or that a business has a reasonable belief is available to the public through widely distributed media.
- Employee data
  - Personal information collected for commercial or business-to-business purposes (in other words, personal information from someone communicating with your company in a commercial setting; e.g. contact information for someone involved in a commercial negotiation)
  - Personal information collected as part of a clinical trial
  - Sale of information to/from consumer reporting agencies

COMPLIANCE REQUIREMENTS UNDER THE VCDPA

The VCDPA imposes a number of affirmative obligations on businesses, and a company must meet these obligations if it falls within the scope of the VCDPA. Many of these obligations mirror those imposed by other data privacy laws. For example, the Virginia General Assembly drew heavily from the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). Thus, organizations that are already subject to those privacy laws may already be compliant with most of the provisions of the VCDPA, though the VCDPA does include some notable nuances. Key differences are emphasized in this memorandum to allow your company to determine whether any gaps exist in its privacy policies.

Further, with 12 comprehensive state privacy laws now signed into law and several more already introduced as bills in state legislatures, your company should consider creating a privacy program that anticipates new laws, allows for growth, flexibility, and scalability, while handling Virginia's newly set requirements. A company-wide privacy program of this nature will allow your company to quickly adapt to new laws with minimal disruption to operations.

- Consumer rights under the VCDPA

  The VCDPA provides consumers with a number of rights with respect to their data, most of which substantially overlap with other state privacy laws, including the CCPA.

  The VCDPA requires that organizations provide consumers the right to opt-out of the sale of their data, profiling, and targeted advertising. VCDPA also requires that organizations do not process sensitive personal data without an affirmative opt-in from the consumer.

  The VCDPA offers consumers a total of seven rights in relation to the collection and use of their personal data. Under the VCDPA consumers are provided:

    - The right to be informed
    - The right to access
    - The right to correction
    - The right to deletion
    - The right to opt-out
    - The right to appeal
    - The right to data portability
    - The right to non-discrimination

  Once a consumer exercises one of these rights (making a request for access, deletion, etc.), the VCDPA requires that the business responds within 45 days. Businesses can extend their response time another 45 days if necessary, but must notify the consumer.

    - Right to Opt-Out of Data Processing

      Perhaps the most important consumer right afforded by the VCDPA, it allows consumers the right to opt-out of:

- The sale of their personal data
- Profiling (automated processing to determine/evaluate information about an individual)
- Targeted advertising

For further clarity of this right, the VCDPA defines the sale of personal data as "the exchange of personal data for monetary consideration by the controller to a third party."

Profiling is defined as any automated processing that evaluates, analyzes, or predicts elements of an individual's economic situation, health, interests, behavior, location, or movements, among other things.

The VCDPA defines targeted advertising as displaying advertisements to a consumer based on personal data obtained from that consumer's activities across websites or applications to predict preferences or interests.

Importantly, the VCDPA explicitly excludes certain advertising activities from the definition of targeted advertising. These include:

- Advertisements based on activities within a controller's own websites or online applications
- Advertisements based on the context of a consumer's current search query, visit to a website, or online application
- Advertisements directed to a consumer in response to the consumer's request for information or feedback
- Processing personal data processed solely for measuring or reporting advertising performance, reach, or frequency

- Right To Appeal and Other VCDPA Consumer Rights

In addition to the right to opt-out of data processing, the VCDPA also provides consumers with the right to be informed about their data, access their data held by an organization, correct and delete that data, and appeal any denial of the consumer's request to exercise their data rights. For your company, this means implementing processes for consumers to exercise these rights. Establishing user-friendly processes that allow consumers to exercise these rights, establishing a formal appeal process, and explaining these rights within your privacy statement will achieve compliance with these VCDPA requirements.

The right to appeal an organization's denial of their data request is a unique aspect of the VCDPA, compared to other comprehensive privacy laws. The VCDPA requires that the appeal process:

- Include an interface that is easy to find and use
- State a fixed time period for your company's response
- Provide a way to contact the Virginia attorney general if your company denies the appeal

Information about how to submit an appeal also needs to be included in your company's privacy policy, as explained in Subsection "E" below.

- Sensitive Data

A key feature of the VCDPA that distinguishes it from other privacy laws (the CCPA in particular), is that an organization may not process "sensitive data" without affirmative consent from the consumer. While the VCDPA is generally more business-friendly than other state privacy laws, the VCDPA is more stringent in its treatment of sensitive data. Unlike the VCDPA's treatment of personal information (and CCPA's treatment of sensitive data) which allows collection unless the consumer opts-out, sensitive data may not be processed under the VCDPA unless the consumer opts-in and consents to the processing.

The text of the law highlights several examples of the type of personal data categorized as sensitive data:

  - Racial or ethnic origin
  - Religious beliefs
  - Mental or physical health diagnosis
  - Sexual orientation
  - Immigration or citizenship status
  - Genetic or biometric data
  - Personal data of a known child
  - Precise geolocation data

Organizations that process sensitive data must obtain valid, affirmative consent (opt-in) from the individual prior to processing this data.

The distinction between personal data (may be processed unless opt-out) and sensitive data (may not be processed unless opt-in) is critical. This feature of the VCDPA demonstrates the importance for your company to know its data - an organization cannot comply with this provision without knowledge of exactly what data is being collected. If your company processes sensitive data, you must be sure to obtain consent prior to processing.

Upon determining whether your company in fact processes any sensitive data, you should consider whether it has a need to process any of this data. Unless it is vital for your company to collect this type of data, avoiding collection of sensitive data altogether is often the best and simplest approach.

- Valid consent

There are two situations in which a company, if subject to the VCDPA, must obtain valid consent from the consumer. First, as discussed above, consent must be obtained by data controllers intending to process sensitive data.

Second, the VCDPA prohibits processing personal information where the purposes of processing are neither reasonably necessary nor compatible with the originally disclosed purposes, unless the consumer's valid consent is first obtained.

> Therefore, while the VCDPA generally requires that processing be reasonably necessary and compatible with the originally disclosed purposes (see Section I of this memorandum), valid consent from the consumer allows the organization to exceed this limitation.

The VCDPA defines consent as "a clear affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement to process personal data relating to the consumer." Valid consent can be obtained in writing or via electronic methods.

- Data Protection Assessments

Under the VCDPA, organizations are required to conduct data protection assessments[ii] in certain circumstances or when certain types of personal data are involved.

Organizations must conduct a data protection assessment in the following scenarios:

  - Processing personal data for the purposes of targeted advertising
  - Selling personal data
  - Processing personal data for the purposes of profiling
  - Processing sensitive data
  - Processing that presents a heightened risk of harm to consumers

When conducting a data protection assessment, an organization must create a clear, documented structure for balancing the benefits to the business against the risk to individuals' privacy. Assessments should include information relating to the context of the processing and the relationship between the data controller and the consumer. Organizations must also document the use of de-identified data as well as the reasonable expectations of the consumer. Organizations do not have to submit assessment documentation to the Office of the Attorney General, but must provide this documentation if requested.

The VCDPA permits use of a single data protection assessment to address a "comparable set of processing operations." Similarly, data protection assessments conducted in compliance with other laws may be deemed acceptable under the VCDPA if the assessment has a "reasonably comparable scope and effect." In other words, a single assessment may be utilized for multiple operations and purposes.

To optimize effectiveness, data protection assessments should be cross-functional, meaning all relevant internal actors from across the company – employees in various departments/sections of the company – should be involved.

Assessments apply only to processing activities after January 2023 and are not retroactive.

- Privacy notices

Privacy notices under the VCDPA must be reasonably accessible, clear, and meaningful. When presenting a privacy notice to an individual, the data controller must include:

  - Categories of personal data being processed
  - Purposes of processing
  - Information relating to how individuals can exercise their rights
  - Information related to how an individual may appeal a decision made in relation to a privacy request
  - Categories of data shared with third parties

- Third parties that personal data is shared with

In relation to consumer rights, data controllers must present consumers with at least one secure method for them to exercise their rights. Data controllers cannot require a consumer to create a new account in order to exercise these rights.

- Third-Party (Processor) Contracts

Most organizations share their data with third-party vendors. Often, these third-parties are "processors" – entities which do not determine the means and purpose of processing but instead follow instructions from the controller. Requirements for transferring personal data to third-parties are common to all state data privacy laws. Thus, regardless of whether your company is subject to the VCDPA specifically, careful selection of vendors and oversight of their data privacy practices is critical.

Under VCDPA, this data sharing relationship must be governed by a detailed contract—one that covers how the data should be processed and requirements applicable to both parties. Specifically, the VCDPA requires a binding contract that states:

- Instructions for processing data
- The nature and purpose of processing
- The type of data subject to processing
- The duration of processing
- The rights and obligations of both the controller and processor

The contract also needs language that specifically governs the data processor's actions, requiring that:

- Any person processing personal data must keep the data confidential
- Data must be deleted or returned at the data controller's request and at the end of the contract
- The processor will provide proof of compliance with privacy obligations, if requested by controller
- The processor will cooperate with compliance audits
- Ensure all subcontractors processing personal information have a written contract with the processor, extending the processor's privacy obligations to the subcontractor.

- Breach Notification and Security Requirements

The VCDPA does not have a mandatory breach notification requirement. However, the VCDPA requires that organizations must "establish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data. Such data security practices shall be appropriate to the volume and nature of the personal data at issue." Va. Code § 59.1-578(A)(3).

No specific controls are required, however the VCDPA's language is similar to the security requirements found in the GDPR and CCPA. There are several places that your company can look to for best practice guidance, including NIST SP 800-53, the Center for Internet Security Critical Security Controls, and the Cloud Controls Matrix of the Cloud Security Alliance.

ENFORCEMENT AND PENALTIES

Compliance with the VCDPA, and good data privacy practices generally, will develop consumer trust through transparent and informed data use. Moreover, compliance with the VCDPA will also help avoid monetary penalties, injunctive actions, and other forms of enforcement.

The VCDPA is enforced by the Virginia Attorney General ("AG"). Unlike the CPRA there is no provision for the establishment of an independent regulator.

The AG has the authority to issue monetary penalties of up to $7,500 per violation of the VCDPA. The AG can also recover reasonable expenses related to the costs involved in investigating violations, including attorney's fees.

While the VCDPA lacks a private right of action, and therefore lacks the teeth that some other state data privacy laws have, the loss of trust from consumers and business partners is a major reason for compliance. In other words, even if violations result in relatively modest fines, the optics of committing VCDPA violations will result in tangible economic and reputational damage.

Importantly, and unlike other state privacy laws, the VCDPA expressly states that there is no private right of action for violations of the law.

The AG will have the ability to issue a notice of violations to businesses that are found to have breached the requirements of the VCDPA. Businesses in receipt of such notice will have 30 days to remedy any violation and report back to the AG confirming that alleged violations have been cured and mechanisms are in place to prevent further violations. This cure period is one of the more business-friendly provisions found in any of the new data privacy laws and provides some respite for businesses hurrying to comply with the new VCDPA requirements.

---

[i] While the VCDPA regulates all forms of consumer data at the state level, consumer credit is regulated federally by the Fair Credit Reporting Act (FCRA) and financial information is regulated by the Gramm-Leach Bliley Act (GLBA), which preempt the VCDPA. The VCDPA specifically carves out exemptions for information subject to GLBA, FCRA, and other sectoral laws regulating data and personal information.

[ii] Referred to as privacy impact assessments ("PIA") in other privacy laws, like the GDPR.