ICBA
One Mission. Community Banks.®

A Guide for Community Banks on Data Privacy Laws and Regulations

Contact:

Lance Noggle
Senior Vice President, Operations Regulatory Counsel
Lance.noggle@icba.org

866-843-4222
icba.org

1100 New York Avenue NW
Suite 500 East
Washington, DC 20005

518 Lincoln Road
P.O. Box 267
Sauk Centre, MN 56378

Introduction

Today's online-centric world reinforces the issue of data privacy. Through state, national, and international laws, policy makers have signaled their desire to protect consumers' privacy in the digital space and enforce penalties on companies who violate this privacy. This guide will walk community banks through some of the more prominent data privacy laws in effect and will be updated as new laws are passed which may impact community banks.

A Title V of the Gramm-Leach-Bliley Act and Regulation P

The Gramm-Leach-Bliley Act ("GLBA"),[1] a comprehensive consumer protection bill passed on November 12, 1999, and its implementing regulations require financial institutions to explain their information sharing practices and protect consumers' sensitive data. Regulation P, more specifically, outlines the requirements for the treatment of nonpublic personal information about consumers by requiring financial institutions to:

- Provide notice to customers about its privacy policies and practices;
- Describe the conditions under which a financial institution may disclose nonpublic personal information about consumers to nonaffiliated third parties; and
- Provide a method for consumers to prevent a financial institution from disclosing that information to most nonaffiliated third parties by "opting-out" of that disclosure.[2,3]

Key Definitions

- **Affiliate** – Any company that controls, is controlled by, or is under common control with another company.
- **Customer** – A consumer who has a customer relationship with you.
    - **Customer relationship** – A continuing relationship between a consumer and you under which you provide one or more financial products or services to the consumer that are to be used primarily for personal, family, or household purposes.
    - **Continuing Relationship** – A consumer has a continuing relationship with you if the consumer:
        - Has a deposit or investment account with you;
        - Obtains a loan from you;
        - Has a loan for which you own the servicing rights;
        - Purchases an insurance product from you;

[1] https://www.govinfo.gov/content/pkg/PLAW-106publ102/pdf/PLAW-106publ102.pdf
[2] https://www.consumerfinance.gov/rules-policy/regulations/1016/1/
[3] Subject to exceptions in §§1016.13, 1016.14, and 1016.15

        - Holds an investment product through you, such as when you act as a custodian for securities or for assets in an Individual Retirement Arrangement;
        - Enters into an agreement or understanding with you whereby you undertake to arrange or broker a home mortgage loan for the consumer;
        - Enters into a lease of personal property with you; or
        - Obtains financial, investment, or economic advisory services from you for a fee.
    - **No continuing relationship** – A consumer does not, however, have a continuing relationship with you if:
        - The consumer obtains a financial product or service only in isolated transactions, such as using your ATM to withdraw cash from an account at another financial institution or purchasing a cashier's check or money order;
        - You sell the consumer's loan and do not retain the rights to service that loan; or
        - You sell the consumer airline tickets, travel insurance, or traveler's checks in isolated transactions.

- **Personally identifiable financial information** – Any information:
    - A consumer provides to a bank to obtain a financial product or service;
    - About a consumer resulting from any transaction involving a financial product or service between you and a consumer; or
    - A bank otherwise obtains information about a consumer in connection with providing a financial product or service to that consumer.

- **Nonpublic personal information** – Personally identifiable financial information; and any list, description, or other grouping of consumers' information (and publicly available information pertaining to them) that is derived using any personally identifiable financial information that is not publicly available.
    - **Nonpublic personal information does not include**:
        - Publicly available information, with some exceptions;[4] or
        - Any list, description, or other grouping of consumers' information (and publicly available information pertaining to them) that is derived without using any personally identifiable financial information that is not publicly available.

[4] Except as included on a list described in paragraph (p)(1)(ii)

- **Publicly available information** – Any information that you have a reasonable basis to believe is lawfully made available to the general public from:
    - Federal, state, or local government records;
    - Widely distributed media; or
    - Disclosures to the general public that are required to be made by Federal, state, or local law.

Major Provisions

Regulation P establishes the treatment of nonpublic personal information about consumers by financial institutions by requiring a privacy notice to customers about the privacy policies and practices of the financial institution. The regulation also describes the conditions under which a financial institution may disclose nonpublic personal information, and how consumers may opt-out of that disclosure.[5]

Providing Notice

Three factors determine when financial institutions must provide notice of their privacy policies. These include:

- An initial notice to an individual who becomes your customer, no later than when you establish a customer relationship, and to a consumer before you disclose any nonpublic personal information about the consumer to any nonaffiliated third party.
- A notice for revisions to the privacy policy. Financial institutions may not share any nonpublic personal information unless consumers are provided a revised notice, have been provided a new opt-out notice with a reasonable opportunity to opt-out, and the consumer does not opt-out.
- In some instances, an annual notice to customers.[6] Annually, in this case, being at least once in any 12 consecutive months.

Notice Requirements

Notices must include:

- Categories of nonpublic personal information collected.
- Categories of nonpublic personal information disclosed.
- Categories of affiliates and nonaffiliated third parties to whom you disclose nonpublic personal information.

[5] Subject to exceptions in §§1016.13, 1016.14, and 1016.15.

[6] Financial institutions are excepted from sending annual notices if they meet the following requirements: a financial institution must not share nonpublic personal information about customers except as described in certain statutory exceptions, and the financial institution must not have changed its policies and practices with regard to disclosing nonpublic personal information. https://www.govinfo.gov/content/pkg/FR-2018-08-17/pdf/2018-17572.pdf

- Categories of nonpublic personal information about former customers disclosed and the categories of affiliates and nonaffiliated third parties to whom you disclose nonpublic personal information about your former customers.
- Explanation of the consumer's right to opt-out of the disclosure of nonpublic personal information to nonaffiliated third parties, including the method(s) by which the consumer may exercise that right at that time.
- Disclosures made under the Fair Credit Reporting Act[7] (that is, notices regarding the ability to opt-out of disclosures of information among affiliates).
- Policies and practices with respect to protecting the confidentiality and security of nonpublic personal information.

Exceptions to the opt-out requirement:
Exceptions to the opt-out requirement exist for service providers and joint marketing agreements as well as for processing and servicing transactions.

When a bank provides nonpublic personal information to a nonaffiliated third party to perform services on their behalf, the opt-out requirements to not apply if, the initial notice is provided in accordance with the notification requirements, and a contractual agreement with the third party prohibits the third party from disclosing or using the information for any other purposes.

Additionally, opt-out and notice requirements do not apply to any transactions made at the consumer's request if a bank discloses nonpublic information as necessary to complete the transaction. This includes servicing or processing a financial product or service that a consumer authorizes, maintaining or servicing the consumers account with the bank or with another entity as part of a private label credit card program or a proposed or actual securitization, secondary market sale, or similar transaction related to a transaction of the consumer.

[7] Section 603(d)(2)(A)(iii)

The General Data Protection Regulation

The European Union ("EU") implemented the General Data Protection Regulation ("GDPR" or "Regulation")[8] on May 25, 2018, which dictates how businesses handle personal data of EU citizens and data subjects. In the EU, a regulation that is passed by the European Parliament and European Commission has direct legal effect throughout the EU. This Regulation replaces the 1995 "Data Protection Directive" ("Directive 95/46/EC").[9]

Paramount to the GDPR is the EU legislative bodies' firm belief that data about an individual belongs to the individual and not to the business that collects the data about the individual, called data controllers. The individual has a right to the data and the individual, through control and deletion of their data, has a "right to be forgotten" (i.e., the individual has a right to privacy). That individual also has a right to obtain their data and take their data to another business. GDPR is wide-ranging and applies to companies within EU member states and businesses across the globe. While the application of EU GDPR for community banks may be limited, it is important to understand what GDPR is, why it is being implemented, and some key elements of the Regulation. ICBA has published a guide to GDPR for community banks, available here.[10]

Key Definitions

- **Personal Data** – Any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.
- **Sensitive Personal Data** – Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, data concerning health or sex life and sexual orientation, genetic data, or biometric data. Data relating to criminal offences and convictions are addressed separately (as criminal law lies outside the EU's legislative competence).

Major Provisions

Data Protection Principles

GDPR outlines protection and accountability principles which data controllers must abide by:

- Processing data must be lawful, fair, and transparent to the EU citizens.

---

[8] https://gdpr-info.eu/

[9] Blackmer, W. Scott. Info Law Group, LLP. https://www.infolawgroup.com/2016/05/articles/gdpr/gdpr-getting-ready-for-the-new-eu-general-data-protection-regulation/ 5 May 2016.

[10] https://www.icba.org/docs/default-source/icba-cyber-secure/cyber-data-security/18-05-23_-eu_gdpr_summary.pdf

- Processing data must be done for the legitimate purposes specified explicitly to the data subject when it was collected.
- Only the absolute minimum amount of data necessary for the purposes specified should be collected.
- Personal data must be kept accurate and up to date.
- Personally identifying data may only be stored for as long as necessary for the specified purpose.
- Processing must be done in such a way as to ensure appropriate security, integrity, and confidentiality.
- Data controllers are responsible for being able to demonstrate GDPR compliance with all principles.[11]

Applicability

GDPR applies to "a company or entity which processes personal data as part of the activities of one of its branches established in the EU, regardless of where the data is processed; or, more likely relevant to U.S.-based community banks, a company established outside the EU offering goods/services (paid or for free) or monitoring the behavior of individuals in the EU."[12] The regulation has a broad territorial scope. It applies to a controller or processor:

- Established in the EU;
- Not established in the EU but offering goods or services to citizens in the EU; or
- Not established in the EU but monitoring behavior of citizens in the EU.[13]

While a community bank may be established to serve a small area, or a targeted area of consumers within the United States and likely without branches outside of U.S. borders, some community banks' customers may be EU citizens or travel, study, or vacation within the EU. If the bank tracks the data of the individual while they are in the EU (i.e. by tracking a customer using website cookies), the bank may also be subject to provisions of GDPR. If the bank does engage in this activity, the bank may want to consider reviewing its disclosures specific to these customers.

Compliance

A community bank with EU citizens or American customers with a presence in the EU should conduct a risk assessment determining whether the bank is offering services to customers in

---

[11] https://gdpr.eu/what-is-gdpr/

[12] European Commission. https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/application-regulation/who-does-data-protection-law-apply_en

[13] KL Gates, "The new General Data Protection Regulation: Global impact, more duties, higher sanctions". http://www.klgateshub.com/files/Uploads/Documents/ACC_Webinar_GDPR_Final.pdf. Page 8. 24 May 2017.

the EU. If the bank contemplates offering services to EU citizens, then the bank may most likely be subject to the provisions of the GDPR.

If a bank determines it is likely subject to EU GDPR following a risk assessment, the bank should review its privacy and data collection disclosures. GDPR requires that, rather than assuming customers consent to the bank's privacy policy, customers must actively agree to very specific data collection policies. GDPR is very clear on this point:

> ***"Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them.***
> ***If the data subject's consent is to be given following a request by electronic means,***
> ***the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided."***[14]

Additionally, if a bank determines it must comply with GDPR, the bank should consult with competent counsel as there are several additional conditions required for compliance with the regulation, such as adherence to the rights of the data subject, including, but not limited to:

- Breach notification;
- The right to access whether data is being processed by a data controller,
- The right to be forgotten (data erasure);
- Data portability (i.e. the ability of the data subject to receive personal data concerning them and the right to transmit that data to another controller); and
- Privacy by design (i.e. including data protection from the onset of designing systems rather than adding data protection after the system is designed).

Data processors are required to maintain certain records and employ a data protection officer.

Noncompliance with the regulation can be costly. The supervisory authority in Europe (The

[14] http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf.

Information Commissioner's Office) can impose sanctions and other corrective measures before assessing fines. However, administrative fines may also be imposed at two levels. The first is up to €10M, or 2% annual global turnover (whichever is greater) or up to €20M, or 4% of annual global turnover (whichever is greater).

Data Breach

In the event of a data breach, the GDPR requires the entity to report a "personal data breach" within 72 hours of becoming aware of the breach. The GDPR defines personal data as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data, transmitted, stored or otherwise processed.

The California Consumer Privacy Act

Similar to the European Union's General Data Protection Regulation ("GDPR"), the California Consumer Privacy Act[15] ("CCPA"), which went into effect January 1, 2020, states that data belongs to the individual and not to the business which collects the data. Additionally, CCPA protects consumers from having their personal information shared without their knowledge. Four central rights are explicitly given to California consumers in the CCPA: the right to know, the right to delete, the right to opt-out, and the right to non-discrimination. While the protections and rights are only granted to California residents, the CCPA may still apply in certain circumstances to community banks outside of California that conduct business with a California resident.

Key Definitions

- **Personal information** – The CCPA has a broad definition of personal information defined as "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. This includes, but is not limited to, the following:
    - Identifiers such as 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.
    - Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.
    - Biometric information.

[15] https://leginfo.legislature.ca.gov/faces/codesdisplayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5

- Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an internet website, application, or advertisement.
- Geolocation data.
- Audio, electronic, visual, thermal, olfactory, or similar information.
- Professional or employment-related information.
- Education information.[16]
- Inferences drawn from any of the information identified in this definition to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.[17]

- **Business** – A business covered by the CCPA must operate for-profit, does business in California and meets any of the following:
  - Have a gross annual revenue of over $25 million;
  - Buy, receive, or sell the personal information of 50,000[18] or more California residents, households, or devices; or
  - Derive 50% or more of their annual revenue from selling California residents' personal information.[19]
- **Doing Business in California** – Unfortunately, doing business in California is not defined by the CCPA. Generally speaking, very basic business interactions with California residents are covered by the CCPA, regardless of whether the resident is a bank customer. For example, while a bank may traditionally consider customers to only be those consumers to which they are providing financial products or services, any collection of personal information of a California resident would trigger CCPA coverage. This could be as simple as collecting IP addresses or other website interaction data for marketing purposes.

Applicability

As mentioned, the CCPA only applies to for-profit businesses, including banks, that do business in California and meet certain requirements.

As most banks will meet one of those criteria, your bank may be impacted depending on whether you do business with a California resident and the information you collect on them. If your bank "does business" with any California residents, whether your bank's operations are

[16] Education information is 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. Sec. 1232g; 34 C.F.R. Part 99).
[17] http://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5
[18] Amended to 100,000 by the California Privacy Rights Act.
[19] https://oag.ca.gov/privacy/ccpa

physically located in California, there is a good chance CCPA will have an impact.

Exemptions

While the CCPA does not provide an entity level exemption for financial institutions regulated by the GLBA, it does provide an information level exemption for personal information that is subject to the GLBA as well as information covered by the Fair Credit Reporting Act ("FCRA"). The CCPA provides an exemption on information "collected, processed, sold, or disclosed pursuant to the GLBA, and implementing regulations." However, the CCPA covers a broader set of transactions with consumers than GLBA.

For community banks, this means that personal information covered under GLBA is exempt from CCPA; however, there may be additional information banks are collecting which are not covered by GLBA but is covered under the broader definition of personal information found in the CCPA. This includes, but is not limited to:

- Consumers not covered by the GLBA. Consumers, and their personal information, who interact with a bank but are not seeking or obtaining consumer financial products or services are not considered "consumers" and, therefore, exempt under GLBA but are covered by CCPA. This includes all personal information as defined by CCPA for such consumers.
- Personal information obtained from non-financial institution partners. Any personal information collected by any source outside of providing consumer financial products and services could be subject to CCPA.
- Information outside the scope of GLBA, such as IP addresses and web identifiers, as well as geolocation data.

Compliance

Community banks who do business with residents of California or collect information from residents of California may be required to follow the CCPA and its regulations.[20] Community banks who believe they are subject to CCPA should review their privacy and data collection disclosures to identify areas where they may already meet the CCPA requirements and areas which may need to be changed to ensure compliance.

Community banks subject to the CCPA must comply with the following:

Notice

The CCPA states that the notice of collection must occur at or before the point of collection

[20] https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/oal-sub-final-text-of-regs.pdf

and shall be designed and presented in a way that is easy to read and understandable to consumers. While there are not required methods of providing notice, it is suggested that a link to the notice be provided on a website's homepage, as well as in printed form in retail locations. The notice must include:

- A list of the categories of personal information about consumers to be collected;[21]
- The business or commercial purposes for which the information will be used;
- A link titled "Do Not Sell My Personal Information" if the personal information is to be sold; and
- A link to the business's privacy policy.

In addition to requiring any community bank subject to CCPA to deliver a notice to California consumers, the CCPA provides these consumers with four privacy rights, for which the bank will need to provide:[22]

- The right to know about the personal information a business collects and how it is used and shared;
- The right to delete personal information collected;
- The right to opt-out of the sale of their personal information; and
- The right to non-discrimination for exercising their CCPA rights.

The Right to Know

Consumers may request that businesses disclose to them what personal information they have collected, used, shared or sold about them, and why they collected, used, shared or sold that information. Any community bank subject to CCPA would be required to provide, at a minimum, a toll-free number and a second method which must be via website, if the community bank has a website for consumers to submit their requests. Community banks have the option of providing more than two options (e.g., email, website form, hard copy form) for consumers to submit their requests, and any request must be responded to within 45 days.

The Right to Delete

CCPA provides consumers with the option to request that businesses delete personal information they collected and instruct their service providers to do the same. Community banks subject to CCPA have 10 days to confirm receipt of the request and 45 days to comply with the request. Banks must provide two methods for consumers to submit requests, but do not have to provide an online form. After receiving the request, a community bank must:

- Permanently and completely erase the personal information on its existing systems with the exception of archived or back-up systems;

[21] As a reminder, information covered by GLBA and the Fair Credit Reporting Act are exempt from the CCPA notice and rights requirements.

[22] https://oag.ca.gov/privacy/ccpa

- Deidentify the personal information; or
- Aggregate the consumer information.

The Right to Opt-Out

CCPA provides consumers with the option to request that businesses stop selling personal information. Community banks subject to CCPA must provide two or more methods for submitting requests and must comply with a request to opt-out "as soon as feasibly possible, but no later than 15 business days from the date the business receives the request." Following a request to opt-out, the community bank may request that consumers opt-in after opting-out, but it must wait 12 months to do so.

The Right to Non-Discrimination

The CCPA dictates that businesses cannot deny goods or services, charge a different price, or provide a different level or quality of goods or services due to a consumer exercising their rights
under CCPA. Businesses can offer consumers promotions or discounts to continue collecting or

selling personal information but do have the right to withdraw the offer if the consumer chooses to opt-out at a later date or have information deleted.

The California Privacy Rights Act

The California Privacy Rights Act[23] ("CPRA") was a ballot initiative in California that passed in November 2020 and took effect in January of 2023. The act amends parts of the CCPA to provide consumers with additional protections – pushing privacy law in California closer to the EU's GDPR. In addition to new consumer protections and updated privacy rights, the CPRA also established the California Privacy Protection Agency ("CPPA") to implement and enforce the new law, while the Attorney General also maintains authority for civil enforcement.

[23] https://www.oag.ca.gov/system/files/initiatives/pdfs/19-0021A1%20%28Consumer%20Privacy%20-%20Version%203%29_1.pdf

Updates

The following table covers major changes or additions to CCPA.

	CCPA	CPRA
Covered Business	For-profit businesses that collect personal information from California residents, determines the purposes in California and meet any of the following: • Have a gross annual revenue of over $25 million; • Buy, receive, or sell the personal information of 50,000 or more California residents, households, or devices; or • Derive 50% or more of their annual revenue from selling California residents' personal information.	For-profit businesses that collect personal information from California residents, determines the purposes in California and meet any of the following: • Have a gross annual revenue of over $25 million; • Buy, receive, or sell the personal information of **100,000** or more California residents, households, or devices; or • Derive 50% or more of their annual revenue from selling California residents' personal information.
Consumer Rights	• Right to Know/Access • Right to Delete • Right to Opt-out of Sale • Right to Non-Discrimination	• Right to Know/Access • Right to Delete • Right to Opt-out of Sale • Right to Non-Discrimination • **Right to Rectification** • **Right to Limit Use and Disclosure of Sensitive Personal Information**
Personal Information	"Information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."	CCPA's definition of personal information, as well as "Sensitive Personal Information" which includes: • Social Security, driver's license, state ID, or passport numbers • Financial account information • Precise geolocation • Racial or ethnic origin • Sex life or sexual orientation • Religious or philosophical beliefs • Union membership • Nonpublic communications (including mail, email, and text content) • Genetic, biometric, and health data
Exemptions	Information level exemption for GLBA and FCRA covered information.	
Data Minimization	Not included	CPRA limits the amount of data a business may collect, use, and share to only the personal information that is reasonably necessary for the purpose of collection.

Dark Patterns	Not mentioned	CPRA states that any agreement "obtained through use of dark patterns does not constitute consent." And defines a dark pattern as "a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision making, or choice, as further defined by regulation." Regulations for CPRA state that consent must be obtained in ways that are easy to understand, have symmetry in choice, do not include confusing or coercive interactive elements, do not contain manipulative language or choice architecture, and are easy to execute.
Enforcement	• California Attorney General • Private Right of Action	• California Attorney General • Private Right of Action • **California Privacy Protection Agency**
Private Right of Action	Only available when the following conditions are met: 1. First and last name are stolen/breached in combination with: a) SSN b) Driver's license number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to identify a person's identity c) Financial account number, credit card number, or debit card number if combined with any required security code, access code, or password that would allow someone access to your account d) Medical or health insurance information e) Fingerprint, retina or iris image, or other unique biometric data used to identify a person's identity (but not including photographs unless used or stored for facial recognition purposes) 2. This information must have been stolen in nonencrypted form and must have been stolen in a data breach as a result of the business's failure to maintain reasonable security procedures and practices to protect it.	

Additional Data Privacy Laws and Regulations

The following list outlines comprehensive data privacy legislation that passed at the state-level, **but either does not apply to community banks or provides exclusions for community banks**. While these laws do not directly impact community banks, they are worth noting as they lay the groundwork for future privacy legislation and may directly impact your bank's customers.

State Name	Year Passed	Effective Date	GLBA Information Level Exemption	GLBA Entity Level Exemption
Colorado	2021	1/1/2023	Yes	Yes
Connecticut	2022	7/1/2023	Yes	Yes
Delaware	2023	1/1/2025	Yes	Yes
Indiana	2023	1/1/2026	Yes	Yes
Iowa	2023	1/1/2025	Yes	Yes
Montana	2023	10/1/2024	Yes	Yes
Tennessee	2023	7/1/2024	Yes	Yes
Texas	2023	7/1/2024	Yes	Yes
Utah	2022	12/31/2023	Yes	Yes
Virginia	2021	1/1/2023	Yes	Yes