SW&M

FINANCIAL INSTITUTION ATTORNEYS

2022 SUMMER LEGAL UPDATE

swmllp.com

Disclaimer

These materials were prepared by the attorneys of Styskal, Wiese & Melchione, LLP. Although this Summer Legal Update was prepared with care, it is not designed to be a complete or definitive analysis of the law in this area. This is a California law specific Summer Legal Update. Laws in other states may vary. Moreover, this Summer Legal Update was prepared with the understanding that it reflects the authors' perception of the state of the law as of this date. Furthermore, the information contained in this Summer Legal Update is not intended to constitute and should not be received as, legal advice and does not in any way create an attorney–client relationship.

SW&M 2022 SUMMER LEGAL UPDATE

Table of Contents

I. INTRODUCTION

While summertime might typically be associated with family vacations, baseball games, and backyard barbecues, summer 2022 may also be memorable for the California Privacy Protection Agency ("Agency") issuing new proposed regulations under the California Privacy Rights Act of ("CPRA"). California financial institutions (as well as those serving significant numbers of California consumers) are painfully aware of the significant changes made to consumers' privacy rights and business' obligations under the California Consumer Privacy Act, which took effect on January 1, 2020. These recently issued proposed regulations under the CPRA will significantly expand upon the consumer protections and rights already applicable under the CCPA. As our financial institution clients may recall from the changes required when the CCPA first took effect, it takes a great deal of time and effort across an institution's various business units to make the necessary changes to its practices and disclosures, as well as working with vendors, to prepare for compliance with the new privacy law.[1] As a result, even though the new CPRA regulations have yet to be finalized, financial institutions should begin preparing for compliance with the CPRA regulations now given the significant changes in privacy practices and disclosures required under the CPRA.

Beyond the CPRA proposed regulations being released, we will discuss other areas affecting financial institutions, including recent noteworthy class action litigation and regulatory agency enforcement action activity, and employment law updates. Below, we have organized the discussion of these legal updates by general area.

II. STATE LAWS AND DEVELOPMENTS THAT APPLY TO FINANCIAL INSTITUTIONS WITH CALIFORNIA OPERATIONS

A. California Privacy Rights Act Update

Background

As you know, the CCPA created an array of consumer privacy rights and business obligations with regard to the collection and sale of personal information, and final regulations issued under the CCPA took effect on August 14, 2020. Although the CCPA and its implementing regulations significantly expanded California consumers' privacy rights, consumer privacy rights advocates were not satisfied. They pursued additional changes, many of them modeled on the rights provided under European Union's General Data Protection Regulation ("GDPR"), through California's ballot initiative process.

On November 3, 2020, California voters approved Proposition 24, enacting the CPRA, which will go into effect on January 1, 2023. As the first comprehensive consumer privacy legislation in the

[1] We should note that the CPRA fortunately retains certain key partial exemptions applicable to financial institution exemptions for certain personal information subject to the federal Gramm-Leach-Bliley Act, the California Financial Information Privacy Act, or the Fair Credit Reporting Act. Since not all personal information collected, used, processed or maintained by financial institutions qualify for these partial exemptions, it is important for financial institutions to seek counsel as to their practices and potential applicability of these exemptions. In addition, CCPA and CPRA apply to businesses that meet certain criteria, i.e., "covered businesses." The criteria under CPRA is different than under CCPA. Our articles are addressed to "covered businesses."

U.S., the CCPA and CPRA may serve as a model for other states and will require companies to evaluate and potentially change the way they do business in California.

On May 27, 2022, the CPPA released proposed regulations to implement the CPRA. This article focuses on the proposed changes to preexisting CCPA requirements by the CPRA regulations. The draft regulations offer businesses a framework for compliance with the CPRA's requirements, such as (for example) obtaining consumer consent to track and share personal data, as well as methods for submitting CCPA requests, new obligations related to "sensitive personal information," pertinent changes applicable to service provider relationships, and changes related to the "workforce data" exception. While it should be noted that the CPRA regulations are only proposed and are subject to revision and finalization, we would also anticipate that most of the proposed regulations will be finalized in a form that materially conforms with the proposed regulations (as was the case for the CCPA final regulations). However, as discussed further below, the CPRA proposed regulations do not cover all twenty-two regulatory rulemaking topics as set forth in Cal. Civ. Code § 1798.185(a).

1. Requirements or Methods for Submitting CCPA Requests and Obtaining Consumer Consent

"Dark Patterns" in Obtaining Consumer Consent

The proposed regulations set forth the basic principles governing the submission of CCPA requests and obtaining consumer consent to collect, share or sell personal information. Generally, businesses must:

(A) Use methods that are easy to understand;

(B) Provide for symmetry in choice;

(C) Not use confusing language and elements;

(D) Avoid manipulative language (including guilting or shaming language) and choice architecture; and

(E) Ensure the methodology is easy to execute by not adding unnecessary burden or friction to the process.

The regulations caution businesses that methods that do not comply with these requirements are "dark patterns." The draft regulations define dark patterns 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." Within the draft regulations are several illustrative examples of dark patterns. One such example provides, "[w]hen offering a financial incentive, pairing choices such as, 'Yes' (to accept the financial incentive) with 'No, I like paying full price' or 'No, I don't want to save money,' is manipulative and shaming."

The draft regulations address the "symmetry in choice" by requiring that a "path for a consumer to exercise a more privacy-protective option shall not be longer than the path to exercise a less

privacy-protective option." An illustrative example in the draft regulations provides, "[a] website banner that serves as a method for opting out of the sale of personal information that only provides the two choices, 'Accept All' and 'More Information,' or 'Accept All' and 'Preferences,'" is not permissible for opting out of the sale or sharing because it requires "the consumer to take additional steps to exercise their right to opt-out of the sale or sharing of their personal information."

While still a draft, the examples highlighted in the regulations indicate that businesses will need to evaluate whether their existing consent and request methodologies may be perceived as dark patterns and how those methodologies can be adapted or revised to comply with the CPRA.

Business Practices for Handling Consumer Requests

Article 3 of the CPRA provides the framework, including the suggested media and prescribed timelines, for processing and responding to requests to delete, requests to correct, and requests to know. Of particular note in Article 3, is that the draft regulations operationalize the CPRA's right to correct inaccurate personal information and right to limit the use of sensitive personal information. The right to correct is an entirely new concept and did not exist in the CCPA.

The regulations provide guidance to businesses on acceptable methods for consumers to submit requests to delete, requests to correct, and requests to know. Specifically, if a business operates exclusively online and has a direct relationship with a consumer, the business may only be required to provide an e-mail address for submitting requests to delete, requests to correct, and requests to know. Otherwise, a business is required to provide two or more designated methods for submitting requests to delete, requests to correct, and requests to know, one of which must be a toll-free telephone number. If the business maintains a website, one of the methods must be through the website such as a webform. Other methods may include, but are not limited to, a designated e-mail address, a form submitted in person, and a form submitted through the mail.

The regulations require a business to consider the methods by which it primarily interacts with consumers to determine which methods to offer a consumer for requests to delete, requests to correct, and requests to know. An illustrative example within the regulations recommends that if the means of interaction with the consumer is in-person, the business should consider providing a pre-printed form that can be directly submitted or sent by mail, a tablet or computer portal that allows the consumer to submit an online form, or telephone number. Accordingly, businesses must consider the primary methods of interactions with their consumers and ensure that they have the appropriate media available for consumers to submit requests to delete, requests to correct, and requests to know.

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

Under the draft regulations, businesses are subject to strict timelines to respond to a request to delete, request to correct, or request to know from consumer and should ensure they have the appropriate internal processes in place to adhere to the statutory requirements. The draft regulations require that within 10 business days a business must confirm receipt of, and provide information about how the business will process, a request to delete, request to correct, or request to know. A business must respond to the request within 45 calendar days after it receives the request. If necessary, a business may take an additional 45 calendar days (for a total of 90 calendar

days) provided the business gives the consumer notice and an explanation of the reason why it will take more than 45 days to respond to the request.

Responding to Requests to Correct

The regulations also operationalize a consumer's right to request a correction of their personal information. This is a new entitlement provided by the CPRA. Upon verification of the consumer's identity, the CPRA requires businesses to determine the accuracy of the contested personal information by considering the totality of the circumstances including the nature of the information, how it was obtained, and documentation relating to the accuracy of the information. A business must accept, review, and consider any documentation that a consumer provides in connection with their request to correct. A business that complies with a consumer's request to correct must correct the personal information at issue and implement measures to ensure that the information remains corrected. Additionally, businesses must also instruct all service providers and contractors to make the necessary corrections. Moreover, businesses must ensure the information remains corrected in their own systems and is not overridden by subsequently received inaccurate information from service providers or contractors such as data brokers. Alternatively, businesses may delete the contested personal information rather than correcting it so long as the deletion does not negatively impact the consumer, or if the consumer consents to the deletion. In responding to a request to correct, businesses must inform the consumer whether they have complied with the consumer's request.

A business may deny a consumer's request to correct if it determines that the contested personal information is more likely than not accurate based on the totality of the circumstances. When denying a consumer's request, the business must explain the basis for the denial, including any conflict with federal or state law, exception to the CCPA, inadequacy in the required documentation, or contention that compliance proves impossible or involves disproportionate effort. If a business claims that compliance would be impossible or involve disproportionate effort, it must provide the consumer with a detailed explanation as to why the business cannot comply with the request.

A business may deny a consumer's request to correct if it denied the same alleged inaccuracy within the past six months. However, the business must treat the request to correct as new if the consumer provides any new or additional documentation to prove the information is inaccurate. A business may also deny a request to correct if it has a good-faith, reasonable, and documented belief the request is fraudulent or abusive. The business must provide the consumer an explanation as to why it believes the information is fraudulent or abusive.

Responding to Requests to Delete

The regulations elaborate on a business's responsibilities when responding to, and expand on a consumer's right to, request their personal information be deleted. Businesses are required to comply with a consumer's request to delete their personal information by permanently and completely erasing the personal information on their own systems (except for archived or back-up systems), deidentifying the personal information, or aggregating the consumer information. Businesses must also notify service providers and contractors to delete the personal information from their records, and notify all third parties to whom the business has sold or shared the information to also delete the information unless this "proves impossible or involves

disproportionate effort." If notifying all third parties would be impossible or involve disproportionate effort, businesses must provide a factual basis for that claim. Significantly, the draft regulations make clear that a business that has failed to put in place adequate processes and procedures to comply with consumer requests cannot claim that responding to a consumer's request requires disproportionate effort. In responding to a request to delete, businesses must inform the consumer whether they have complied with the consumer's request.

If a business denies a consumer's request to delete in whole or in part, the business must explain the basis for the denial, including any conflict with federal or state law, exception to the CCPA, or contention that compliance proves impossible or involves disproportionate effort. If a business claims that compliance would be impossible or involve disproportionate effort, it must provide the consumer with a detailed explanation as to why the business cannot comply with the request. The business must delete, and instruct its service providers and contractors to delete, the personal information that is not subject to the exception and ensure that the retained information is not used for any purpose other than as provided for in the exception.

Responding to Requests to Know

The proposed regulations largely retain the existing CCPA procedural requirements concerning a consumer's request to know. However, there are a few notable additions. Intriguingly, there is an inconsistency between how the statute and the draft regulations treat requests for personal information extending beyond a 12-month period. The language of the statute is permissive allowing that "a consumer ***may*** request that the business disclose the required information beyond the 12-month period." The language of the draft regulations is mandatory requiring that the "business ***shall*** provide all the personal information it has collected and maintains about the consumer on or after January 1, 2022, including beyond the 12-month period preceding the business's receipt of the request" (emphasis added). The draft regulations also remove all other references to the 12-month look-back period for requests to know contained in the existing CCPA regulations. The CPPA does not offer any explanation about why businesses are required to provide information beyond the 12-month period.

As with other CCPA requests, the draft regulations require that if a business claims complying with a consumer's request for information extending beyond the 12-month period would be "impossible or would involve disproportionate effort," the business must "provide the consumer a detailed explanation that includes enough facts to give a consumer a meaningful understanding as to why the business cannot provide personal information beyond the 12-month period." Simply stating that the response would be "impossible" or "require disproportionate effort" would not be sufficient.

Requests to Opt-Out of Sale/Sharing

The regulations address the methods by which a consumer can request to opt-out of the sale and/or sharing of their personal information and a business's obligations upon receipt of such request. The draft regulations require a business to provide at least two methods for opting out of the sale/sharing of personal information. A business must consider the manner in which it interacts with consumers, the manner in which it collects the personal information, available technology, and the ease of use for the consumer to submit an opt-out request. If a business collects information online, it must allow a consumer to opt-out through an opt-out preference signal, through an

interactive form via the "Do Not Sell My Personal Information" link, or through the business's privacy policy. If the business interacts with consumer in person, it may provide an in-person method for submitting opt-out requests. Other acceptable opt-out methods include a toll-free phone number, a designated e-mail address, a form submitted in person or through the mail. Businesses cannot require a consumer create an account or provide additional information beyond what is necessary to initiate an opt-out request. Businesses cannot require a verifiable consumer request for a request to opt-out of sale/sharing. Businesses must cease selling and/or sharing the personal information of the consumer as soon as is feasible but no later than 15 business days from the date it receives the request. Businesses must notify all third parties to whom the business has sold or shared the information that the consumer has made an opt-out request. Businesses must provide a means by which the consumer can confirm their request has been processed by the business. Once a consumer has requested to opt-out, businesses must wait 12 months to consent to the sharing of their personal information.

2. Sensitive Personal Information

CPRA Grants Rights to Limit Use and Disclosure of Sensitive Personal Information

Among the rights the CPRA granted to California consumers was the right to limit the use and disclosure of "sensitive personal information." The new law establishes that a consumer has the "right, at any time, to direct a business that collects sensitive personal information about the consumer to limit its use of the consumer's sensitive personal information to that use which is necessary to perform the services or provide the goods reasonably expected by an average consumer who requests those goods or services…" Once a business receives notification from the consumer that he/she/they wish to exercise this right, it is prohibited from using or disclosing the consumer's sensitive personal information for any other purpose. This addition to California's privacy laws will obligate businesses to initiate policies and processes wherein sensitive personal information is readily identified and separated from other personal information such that a consumer's request to limit the use or disclosure of sensitive personal information is seamlessly resolved. Further, under Senate Bill 1189, the California legislature is considering further restrictions on a particular type of sensitive personal information, biometric information.

Analysis of Key Definitions

Personal Information. Personal information means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked to, the following if it identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household. Note that the definition of personal information includes, but is not limited to, "biometric information" as well as "sensitive personal information." Personal information does NOT include publicly available information, which means that it is lawfully made available from federal, state, or local governments records. Public information also does NOT include consumer information that is "deidentified or aggregate consumer information."

Sensitive Personal Information. Sensitive personal information is specifically defined as:

- Personal information that reveals:
  - Social security, driver's license, state identification card, or passport number;

- 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;
- Precise geolocation;
- Racial or ethnic origin, religious or philosophical beliefs, or union membership;
- Contents of a consumer's mail, email, and text messages unless the business is the intended recipient of the communication; and
- Genetic data.

- The processing of biometric information for the purpose of uniquely identifying a consumer and personal information collected and analyzed concerning either a consumer's health or a consumer's sex life or sexual orientation.

Sensitive personal information does **NOT** include information that is publicly available, as previously defined.

Biometric Information. Biometric information is specifically defined as an individual's physiological, biological, or behavioral characteristics, including information pertaining to an individual's DNA, that is used or is intended to be used singly or in combination with each other or with other identifying data, to establish individual identity. The definition includes, but is not limited to, imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information.

In sum, most any information that identifies an individual consumer is considered personal information under the CPRA; however, only particular data is further defined as sensitive personal information. The CPRA only grants a consumer the right to limit the use or disclosure of data such as a consumer's SSN, passport number, certain protected classes like race, ethnicity, and religion, precise geolocation, genetic data, account information or the processing of biometric information. Senate Bill 1189, if it becomes law, will impose further restrictions on biometric information.

Right to Limit

If a business collects sensitive personal information, the business is required to disclose to the consumer that such data is being collected, the purpose for collecting it, and the consumer's right to limit the business' use of his/her sensitive personal information. The purpose for granting consumers the right to limit is to give consumers meaningful control over how their sensitive personal information is collected, used, and disclosed. While the consumer's right to limit use of sensitive personal information only applies where the business is collecting sensitive personal information with the purpose of "inferring characteristics about a consumer," businesses should not rely on this exception in handling sensitive personal information.

Businesses will need to first evaluate their processes for collecting data from consumers. A business should consider at what points it is collecting sensitive personal information and for what purposes. Then, the business will determine how to categorize and track the data it has collected. For financial institutions, for example, a consumer's social security, driver's license or state identification card numbers are likely collected when a new account is opened or when an

application is submitted for a service or product. Another example would be the collection of precise geolocation technology for antitheft purposes while a consumer is travelling and attempts to access his/her accounts.[2] There are various points during the course of business when sensitive personal information is collected. For the sake of efficiency when complying with a consumer's request to limit the use of sensitive personal information, it is imperative that businesses have processes in place whereby sensitive personal information is easily identified and separated for limited use.

Another aspect of compliance with this new restriction is in determining which uses and disclosures of sensitive personal information the consumer has the right to limit. Once a consumer submits a request to limit use of the sensitive personal information, the business may exclude any use that is "necessary to perform the services or provide the goods reasonably expected by an average consumer." Such usage would not be impacted by a consumer's request to exercise his/her right to limit the business' use of that information. However, if the business uses such information for purposes outside of that exception, such as targeted marketing for other products/services offered by the business or its associates, the consumer would likely have the right to prohibit the business from such use. Accordingly, businesses would be advised to initiate processes by which personal information that is identified as sensitive will only be used for necessary purposes. Businesses should identify exactly which purposes fit within the "necessary" exception and create a process that efficiently removes sensitive personal information for any other purpose outside of the "necessary" exception.

The CPRA's right to limit also requires businesses to provide notice of the right to limit to consumers. While the CCPA already requires a notice at collection, the notice required for sensitive personal information is distinct from the other notices under CCPA. The notice must be reasonably accessible and understandable to consumers. Businesses are required to provide a "clear and conspicuous link" on the business' Internet homepages specifically for consumers who want to limit the use of sensitive personal information.

Biometric Information

In addition to the requirements imposed by the CPRA regarding sensitive personal information in general, the California legislature has proposed SB 1189 which provides stricter requirements for the collection, use, retention and disclosure of biometric information. If enacted, SB 1189 will require businesses to: (1) establish a schedule for the retention and permanent destruction of biometric information; and (2) make the schedule publicly available. SB 1189 would restrict the collection of biometric information without the subject's request or authorization unless the private entity requires it for a "valid business purpose." Further, before collecting the biometric information, the business will be required to inform the subject, in writing, of what biometric information is being collected, stored or used, as well as the purpose of the collection and the length of time for its use. If passed, these additions will go into effect September 1, 2023.

The California legislature's intent is to tightly restrict businesses from profiting from such highly sensitive personal information without the consumer's knowledge and consent. While the CPRA does permit private rights of action against businesses for data breaches, SB 1189 would permit

[2] Note that these examples would likely fall within the Gramm-Leach-Bliley Act exemption under the CPRA for "personal information collected, processed, sold, or disclosed subject to the Gramm-Leach-Bliley Act."

consumers to file a civil suit against businesses for any violation of this title. Unlike the CPRA, violations of SB 1189 could result in punitive damages against the business as well as attorney's fees and statutory damages with higher maximum fines.

Even if SB 1189 does not pass in its current form during this legislative session, businesses can predict that there will be further attempts to restrict the use, sale, disclosure, and retention of biometric data given the precedent set by other states such as Illinois, Texas, and Washington. The State of Illinois, for example, enacted the Biometric Information Privacy Act in 2008 ("BIPA"). Since BIPA was enacted, Illinois federal and state courts have seen hundreds of class action lawsuits against companies allegedly out of compliance with BIPA. Some of these lawsuits have settled out of court for millions. For example, in *Rosenbach v. Six Flags Entm't Corp*, the Illinois Supreme Court concluded that a technical violation of BIPA created a "real and significant injury" in and of itself to consumers. Six Flags subsequently settled the case for $36 million.

As mentioned above, businesses will need to begin initiating processes and procedures in order to ensure compliance with the CPRA regulations now. Notices to consumers will need to be updated with additional information and particular types of personal information will need to be separately collected, retained, and monitored for consumer requests to limit or deny the business' use. Businesses should be aware of when sensitive personal information is collected and for what purposes. Further, businesses will want to begin developing policies for the collection, use, and disclosure of biometric information in particular. However, they should also monitor the status of SB 1189, to ensure that they are prepared to also comply with its requirements if enacted.

3. Data Minimization/Purpose Limitation

Data Minimization

Data minimization is a core concept within the GDPR and the Fair Information Practice Principles, but it was not present in the CCPA. It has now been added via the CPRA. Data minimization is the intentional reduction of data through applying targeted collection methods, only collecting the data that is strictly necessary for the purpose for which it was collected. Specifically, California Civil Code § 1798.100(c) requires that:

> "[a]business' collection, use, retention, and sharing of a consumer's personal information shall be reasonably **necessary and proportionate** to achieve the purposes for which the personal information was collected or processed, or for another disclosed purpose that is compatible with the context in which the personal information was collected, and not further processed in a manner that is incompatible with those purposes."

Cal. Civ. Code § 1798.100(c). In other words, in deciding what information to collect, a financial institution should consider the purpose for which the data is being collected and narrowly tailor the scope of the collection to that purpose. It is the antithesis of an overbroad collection and collection disclosure made "just in case."

Proposed regulation § 7002 deals with data minimization, and provides further explanation of what it means to be reasonably "necessary and proportionate," as required by the language of the statute.

It makes clear that they key to determining what is reasonably necessary and proportionate is what an average consumer would expect, and provides several examples illustrating that concept:

> "(1) Business A provides a mobile flashlight application. Business A should not collect, or allow another business to collect, consumer geolocation information through its mobile flashlight application without the consumer's explicit consent because the collection of geolocation information is incompatible with the context in which the personal information is collected, i.e., provision of flashlight services. The collection of geolocation data is not within the reasonable expectations of an average consumer, nor is it reasonably necessary and proportionate to achieve the purpose of providing a flashlight function.
>
> (2) Business B provides cloud storage services for consumers. An average consumer expects that the purpose for which the personal information is collected is to provide those cloud storage services. Business B may use the personal information uploaded by the consumer to improve the cloud storage services provided to and used by the consumer because it is reasonably necessary and proportionate to achieve the purpose for which the personal information was collected. However, Business B should not use the personal information to research and develop unrelated or unexpected new products or services, such as a facial recognition service, without the consumer's explicit consent because such a use is not reasonably necessary, proportionate, or compatible with the purpose of providing cloud storage services. In addition, if a consumer deletes their account with Business B, Business B should not retain files the consumer stored in Business B's cloud storage service because such retention is not reasonably necessary and proportionate to achieve the purpose of providing cloud storage services.
>
> (3) Business C is an Internet service provider that collects consumer personal information, including geolocation information, in order to provide its services. Business C may use the geolocation information for compatible uses, such as tracking service outages, determining aggregate bandwidth use by location, and related uses that are reasonably necessary to maintain the health of the network. However, Business C should not sell to or share consumer geolocation information with data brokers without the consumer's explicit consent because such selling or sharing is not reasonably necessary and proportionate to provide Internet services, nor is it compatible or related to the provision of Internet services.
>
> (4) Business D is an online retailer that collects personal information from consumers who buy its products in order to process and fulfill their orders. Business D's provision of the consumer's name, address, and phone number to Business E, a delivery company, is compatible and related to the reasonable expectations of the consumer when this personal information is used for the purpose of shipping the product to the consumer. However, Business E's use of the consumer's personal information for the marketing of other businesses' products would not be necessary and proportionate, nor compatible with the consumer's expectations. Business E would have to obtain the consumer's explicit consent to do so."

Purpose Limitation
Purpose limitation is very closely entwined with data minimization. Data minimization requires narrowly tailoring the scope of collection, while purpose limitation requires that the collecting party obtain explicit consumer consent (opt-in) before collecting data which is unrelated to or incompatible with the purpose of collection. If an opt-in is required, then it must be obtained in accordance with proposed regulation 7004. However, collection beyond the immediate need may be made without opt-in (thus going beyond a narrowly tailored collection) so long as the purpose is disclosed and it is compatible with what is reasonably expected by the average consumer.

This can create a challenge for businesses collecting data, and require some thoughtful crafting of disclosures in order to leave some flexibility regarding future needs. For example, if a business is collecting data needed to operate an application, and the application is likely to have functionality in the future that would require additional categories of data, the business may wish to craft a disclosure regarding the additional data, even though it is not strictly needed for the operation of the application at the present time. Of course, it must still be compatible with what is reasonably expected by the average consumer or opt-in would be required.

4. Right to Limit Automated Decision-Making

Pursuant to the CPRA, the Agency, was directed to adopt regulations to further the purposes of the CCPA, including promulgating regulations on 22 specific topics. One of those topics included issuing "regulations governing access and opt-out rights with respect to businesses' use of automated decision-making technology, including profiling and requiring businesses' response to access requests to include meaningful information about the logic involved in those decision-making processes, as well as a description of the likely outcome of the process with respect to the consumer." Notably, the Agency did not address this topic in its preliminary proposed regulations. Nonetheless, this is a critical topic that we expect the Agency to address soon and a topic that will have great significance given the continued prevalence of automated technology in the financial services industry.

Although the current proposed regulations did not address the aforementioned topic, we will address below some practical measures and steps financial institutions may undertake now in preparation for compliance with the new CPRA requirements and the anticipated regulations related to automated decision-making. Additionally, we will discuss the direction the Agency may be headed in promulgating regulations related to automated decision-making.

Steps to Take in Anticipation of the Automated Decision-Making Regulations
As mentioned, the CPRA allows consumers to request information about the logic involved in automated decision-making and a description of the likely outcome of processes with respect to the consumer. The CPRA's description of automated decision-making and the right to opt-out is very broad and the scope of this right will need to be further developed through regulations, including any exceptions to the right of opt-out, such as processing a transaction initiated by the consumer. As financial institutions adopt and integrate new software and technologies in their operations, they must be mindful of fully automated decision-making processes and discuss with vendors what their technological capabilities are to process an opt-out request.

Furthermore, financial institutions must also be mindful of the interplay between automatic decision-making and fair lending considerations, as some algorithms may lead to disparate impacts based on a consumer's protected trait (i.e., race).[3] This concept has garnered significant public commentary at the invitation of the Agency, which will surely promulgate regulations that will hopefully clarify this concept for the industry. Additionally, the CFPB recently opined in its annual fair lending report to Congress on May 6, 2022, that the future of the financial services industry will be increasingly shaped by predictive analytics, algorithms, and machine learning and as such, the CFPB made it clear that one of its main focuses going forward will be analyzing digital redlining and algorithmic biases to identify emerging risks. Although the CFPB recognized the potential positive impact of these technologies for expanding access to credit, it noted that these technologies must be carefully crafted to avoid reinforcing historical biases that have improperly excluded consumers from various lending opportunities.

In addition, the CFPB published a Consumer Financial Protection Circular 2022-03 ("Circular") on May 26, 2022, to remind financial institutions of their obligations under the Equal Credit Opportunity Act ("ECOA"), as implemented through Regulation B, regarding adverse action notices even when algorithms or automated models are used in the decision-making process. This Circular ties in nicely with the pending regulations as it reiterates the fact that financial institutions are already obligated to provide statements of specific reasons to applicants against whom adverse action is taken, even where the decision was made via an automated process. These adverse action notice requirements under the ECOA/Regulation B appear to have some similarities to the CPRA requirements, in that the CPRA will require the provision of meaningful information about the logic involved in the automated decision-making process. However, we currently do not know how much information a financial institution will need to provide for it to be considered "meaningful information" per the CPRA; this should be addressed in the forthcoming regulations.

Having said that, and although it is currently unknown to what extent financial institutions will need to explain the logic involved in their automated decision-making processes under the CPRA, the CFPB was clear as to the expectation under the ECOA/Regulation B. In this regard, the CFPB noted in its Circular that the obligation to provide specific reasons for adverse action per the ECOA/Regulation B prohibits financial institutions from using complex algorithms when doing so means they cannot provide specific and accurate reasons for adverse action. According to the CFPB, whether a creditor is using a sophisticated machine learning algorithm or more conventional methods to evaluate an application, the legal requirement is the same under the ECOA: creditors must be able to provide applicants against whom adverse action is taken with an accurate statement of reasons. The statement of reasons "must be specific and indicate the principal reason(s) for the adverse action."

Based on the foregoing, and if the Agency follows the same principles outlined by the CFPB in its Circular, financial institutions could potentially be prohibited from using complex algorithms if doing so would prevent them from being able to provide meaningful information about the logic of their automated decision-making process. As such, financial institutions should continue to identify the reasons relied upon in its automated decision-making since it is already required under

[3] As mentioned above, there are certain exemptions under the CCPA that may be applicable, depending on factors such as the institution's practices and the nature of the information involved.

the ECOA/Regulation B and will be required under the CPRA (although we do not know to what extent until regulations come out).

Said guidance from the CFPB further solidifies the importance of financial institutions staying fully informed as to any automated decision-making process for compliance with the CPRA and also, as to fair lending issues and inherent biases, which may be easier to track (even for regulators) given the technological capabilities of these systems to store, process, and decipher data. Staying informed will likely require open lines of communication between financial institutions and their vendors/solution providers that provide automated decision-making services.

As part of their due diligence, financial institutions should identify all of the areas in which automated decision-making technologies are deployed in their business processes, evaluate their agreements with such solutions providers to determine whether any information about the logic involved in the decision-making may be disclosed if required by the CPRA, and reach out to such solutions providers to inquire about how they plan on complying with this aspect of the CPRA. Further, indemnification provisions with these vendors/solution providers and the protections provided therein may prove to be important given the unsettled legal landscape as to these newer and advancing technologies.

GDPR and its Potential Application and Effect on the Automated Decision-Making Regulations
Much of the public commentary to the Agency's request for public commentary on the topic of automated decision-making emphasized that the Agency should model its regulations after the GDPR, which already has a relatively established regulatory framework on this topic.

A notable commentator, Alastair A. Mactaggart of the Californians for Consumer Privacy, whose state ballot initiatives in 2018 and 2020 led to the CCPA and the CPRA respectively, requested that the Agency examine this new right in light of GDPR Article 13(2)(f) and 14(2)(g) (both referencing GDPR Article 22) and GDPR Guidelines. Pursuant to the GDPR Guidelines, providing meaningful information about the logic involved in automated decision-making does not necessarily require a complex explanation of the algorithms used or disclosure of the full algorithm. Rather, the information provided should be sufficiently comprehensive for the consumer to understand the reason for the decision.

Based on the foregoing, and given the public commentary, we would not be surprised if the Agency will incorporate a framework similar to the GDPR Guidelines related to automated decision-making into the forthcoming regulations, although it is possible the Agency could take a different approach. Even when these regulations do come out, they may be more susceptible to change as technologies progress over time. Given such fluidity and uncertainty, financial institutions should hone in on their automated decision-making processes and become familiar with such processes so that they can quickly adapt and comply with the legal and regulatory changes.

5. CCPA/CPRA – Workforce Data Exception

When the CPRA takes effect on January 1, 2023, one of the major exceptions to the law is scheduled to expire, leaving employers in California liable for a myriad of additional protections from which they had been previously exempt. As a result, in a few months, businesses may be

subject to all of the CCPA's requirements for disclosure, deletion, and maintenance of employee personal information.

For background purposes, the CCPA was amended in 2019 to grant the Workforce Data Exception to businesses. Under this exception, certain kinds of personal information were excluded from some of the CCPA regulations. Specifically, the exception temporarily exempted covered businesses from CCPA compliance for personal information that is collected about a job applicant, employee, owner, director, officer, medical staff member, or contractor (collectively, the "Workforce"), only when the personal information is collected and used *solely* within the context of that person's role, for that person's emergency contact information, or to administer that person's benefits. While the Workforce Data Exception excluded employers from most of the CCPA regulations, two important obligations remained. Personal information that qualified as workforce data was still subject to two CCPA requirements: (1) employers must still provide notices of collection; and (2) employers must still provide adequate protection of the collected personal information against data breaches.

The Workforce Data Exception was scheduled to expire on January 1, 2021. Thereafter, workforce data would have been subject to the full list of protections and obligations under the CCPA. However, the CPRA extended the Workforce Data Exception's expiration date to January 1, 2023. Businesses are likely to incur significant costs in administering the CCPA (as amended by CPRA) protections to employee personal information. We will discuss how California businesses will be impacted if the Workforce Data Exception of the law either expires or is extended. In either instance, businesses will need to have policies, procedures, personnel, and training that is in alignment with the privacy protections afforded to the workforce.

Proposed Bills – Senate Bill 1454 and Assembly Bill 2891

In February 2022, Senate Bill 1454 was introduced. The bill proposes to extend the Workforce Data Exception indefinitely. The CPRA authorizes the Legislature to amend the act to further the purposes and intent of the act by a majority vote of both houses of the Legislature. The last action taken on this bill was in March 2022. To date, it is still pending.

Also in February 2022, Assembly Bill 2891 was introduced. The bill proposes to extend the Workforce Data Exception until January 1, 2026. This bill also claims to be in furtherance of the purposes and intent of the CPRA. The last action taken on this bill was in March 2022. To date, it is still pending.

Given the extensive protections that would be afforded to a company's workforce if the exception does expire under the current law, businesses may consider, sooner rather than later, preparing to implement policies and procedures in order to comply. Whether the proposed extensions of the Workforce Data Exception pass or not, effective January 1, 2023, businesses will need to revise existing privacy policies and procedures and/or implement additional ones by January 1, 2023, because the CPRA requires including additional information in such disclosures and the Workforce Data Exception does not exempt employers from providing the notice at collection required under the CPRA.

Once the CPRA becomes effective, the requirements for the notice at collection are expanded (even if the California legislature extends the Workforce Data Exception's expiration date). The CPRA will require employers to also disclose to the employee whether their personal information is sold or shared and the retention period for each category of personal information collected. In addition, the CPRA mandates a distinction between "personal information" versus "sensitive personal information."[4] Businesses are prohibited from retaining a consumer's personal information for longer than is "reasonably necessary for that disclosed purpose."

The requirement to protect an employee's data from unauthorized access and exfiltration, theft, or disclosure is consistent in both the CCPA and the CPRA with a minor exception.[5] Overall, employers bear the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect it.

The remainder of this section will discuss how the CPRA will affect workforce data collection and use during hiring, onboarding, and active employment if the Workforce Data Exception is **not** extended.

What if neither bill passes?

In the event that neither of the proposed bills to extend the expiration of the Workforce Data Exception are passed, businesses should be prepared to ensure compliance with the entirety of the CCPA as amended. While the exemption is in place, employers are able to forego all but 2 of the requirements mandated by the CCPA. As the law currently stands, this exemption will expire on January 1, 2023 and the full law will become applicable to workforce data collected by employers.

Upon expiration of the Workforce Data Exception under the CCPA as amended by the CPRA, the obligations for which employers would be include:

- The obligation to inform consumers of their right to request that a business delete any personal information about the consumer which the business has collected from the consumer. Upon such request from a consumer, businesses must delete the information and direct any service providers and third parties to delete the information;
- The obligation to disclose to the consumer the specific pieces of personal information it has collected about that consumer. The business is further obligated to permit the consumer to access to his/her personal information that the business has collected;
- The obligation to notify consumers of their right to opt out of the sale or sharing of their personal information to third parties. Businesses are further obligated to refrain from selling a consumer's personal information when the consumer has requested to opt out;
- The obligation to refrain from selling the personal information of consumers less than 16 years of age unless the consumer or the consumer's parent or guardian affirmatively authorizes the sale of the data;

[4] Sensitive personal information includes, but is not limited to, an employee's social security, driver's license, state ID card, or passport number, credentials for accessing accounts, racial or ethnic origin, religious or philosophical beliefs, or union membership, genetic data, biometric information, etc.

[5] The CPRA, in addition to nonencrypted and nonredacted personal information, added an employee's email address in combination with a password or security question and answer. If such information is subject to unauthorized access, etc., the employer is liable for a civil action.

- The obligation to not discriminate against any consumer for exercising any of the above rights; and
- The obligation to correct inaccurate personal information upon request from the consumer.

With so many new obligations, various departments within a business will need to review its policies and procedures for collecting and using an employee's personal information.

6. Third-Party & Vendor Management Considerations For Service Providers, Contractors, And Third-Parties

Under the CCPA, there were only two categories of data recipients from a covered business: "service providers" and "third-parties." The CPRA and the proposed regulations create a new category called "contractor." The CPRA and proposed regulations attempt to draw clear distinctions among these categories and provide prescriptive contractual requirements for a covered business' contracts with such parties.

Analysis of Key Definitions

Service Provider. A service provider is defined as a person that processes[6] personal information on behalf of a business and that receives from or on behalf of the business a consumer's personal information for a business purpose pursuant to a written contract, provided that the contract prohibits the person from:

(A) Selling or sharing the personal information;

(B) Retaining, using, or disclosing the personal information for any purpose other than for the business purposes specified in the contract for the business, including retaining, using, or disclosing the personal information for a commercial purpose other than the business purposes specified in the contract with the business;

(C) Retaining, using, or disclosing the information outside the direct business relationship between the service provider and the business; and

(D) Combining the personal information that the service provider receives from, or on behalf of, the business with personal information that it receives from, or on behalf of, another person or persons, or collects from its own interaction with the consumer.

Contractor. The CPRA defines a contractor as a person to whom the business makes available a consumer's personal information for a business purpose, pursuant to a written contract with the business. The written contract requirements are nearly identical to the requirements for service providers. However, the definition of a "contractor" is broader as it is any person to whom a business makes available personal information for a business purpose, compared to a "service provider" who must process the information on behalf of a business. Another distinction is that a contractor must receive personal information directly from the business, while a service provider may receive personal information "from or on behalf of the business."

[6] Processing means any operation or set of operations that are performed on personal information or on sets of personal information, whether or not by automated means.

Third-Party. Under the CPRA, a "third party" is now any person who is not any of the following:

- The business that collects personal information from an intentional interaction with the consumer as part of their current business interaction under the CPRA.
- A "service provider" to the business.
- A "contractor."

Service Providers and Contractors

The CPRA also revised provisions relating to the business purposes for which service providers and contractors can process personal information. Prior to the CPRA, transferring personal information or providing access to personal information to service providers is an express exemption to sale if certain criteria are met.

The CPRA rewrote the sections dealing with service providers, sales, and third parties to streamline the language and clarify the exclusions. Under the CPRA:

- Sales only occur when the recipient is a third party, which is a defined term.
- By definition, a business's qualified service providers or contractors are not third parties.

The proposed regulations amend the CCPA by expanding the regulations to apply to contractors and address the revised definition of business purpose.

Use Restrictions

With that, under the proposed regulations, a service provider or contractor shall not retain, use, or disclose personal information obtained in the course of providing services except:

(A) To process or maintain personal information on behalf of the business that provided the personal information or authorized the service provider or contractor to collect the personal information.

(B) For the specific business purpose(s) and service(s) set forth in the written contract required by the CCPA and its regulations.

(C) To retain and employ another service provider or contractor as a subcontractor, where the subcontractor meets the requirements for a service provider or contractor under the CCPA and its regulations.

(D) For internal use by the service provider or contractor to build or improve the quality of its services, provided that the service provider or contractor does not use the personal information to perform services on behalf of another person.

(E) To detect data security incidents or protect against malicious, deceptive, fraudulent, or illegal activity.

(F) For the purposes enumerated in Civil Code § 1798.145, subdivisions (a)(1) through (a)(7), which include:

(i) Complying with federal, state, or local laws or complying with a court order or subpoena to provide information.

(ii) Complying with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, or local authorities.

(iii) Cooperating with law enforcement agencies concerning conduct or activity that the business, service provider, or third party reasonably and in good faith believes may violate federal, state, or local law.

(iv) Cooperating with a government agency request for emergency access to a consumer's personal information if a natural person is at risk or danger of death or serious physical injury (if certain criteria are met).

(v) Exercise or defend legal claims.

(vi) Collect, use, retain, sell, share, or disclose consumers' personal information that is deidentified or in the aggregate consumer information

(vii) Collect, sell, or share a consumer's personal information if every aspect of that commercial conduct takes place wholly outside of California.

The drafters of the proposed regulations deemed the above necessary because it provides clear guidance regarding the interrelationship of the terms "service provider," "contractor," "business purpose," and "commercial purpose" defined in the CCPA. Both a service provider and a contractor are prohibited from using personal information for any purpose other than the business purpose specified in the required written contract, including retaining, using, or disclosing the personal information for a commercial purpose other than the business purposes specified in the contract. The language above clarifies what is and is not an appropriate use of personal information that would advance the commercial purposes of the service provider rather than the business purpose of the business.

Beyond the prohibitions mentioned above, the proposed regulations added new language clarifying that cross-contextual behavioral advertising[7] is not a business purpose for which a service provider or contractor can contract with a business. The reasoning behind this addition was to clarify the new definition of "business purpose," which expressly excludes cross-contextual behavioral advertising from the permitted business purpose of providing advertising and marketing services. In addition to this, a service provider or contractor cannot combine the personal information of opted-out consumers that the service provider or contractor receives from, or on behalf of, the business with personal information that the service provider or contractor receives from, or on behalf of, another person or persons or collects from its own interaction with consumers.

[7] "Cross-context behavioral advertising" means the targeting of advertising to a consumer based on the consumer's personal information obtained from the consumer's activity across businesses, distinctly-branded websites, applications, or services, other than the business, distinctly-branded website, application, or service with which the consumer intentionally interacts.

This is a major revision to the CCPA by the CPRA as a business that contracts with a person to provide cross-contextual behavioral advertising would be a third party and not a service provider or contractor, and in such event, the business would be required to provide consumers with the ability to opt out of the sale or sharing of their personal information for such cross-contextual behavioral advertising. The proposed regulations provided two examples, as follows:

(A) Example 1: Business S, a clothing company, hires a social media company as a service provider for the purpose of providing Business S's advertisements on the social media company's platform. The social media company can serve Business S by providing non-personalized advertising services on its platform based on aggregated or demographic information (e.g., advertisements to women, 18-30 years old, that live in Los Angeles). However, it cannot use a list of customer email addresses provided by Business S to identify users on the social media company's platform to serve advertisements to them.

(B) Example 2: Business T, a company that sells cookware, hires an advertising company as a service provider for the purpose of advertising its services. The advertising agency can serve Business T by providing contextual advertising services, such as placing advertisements for Business T's products on websites that post recipes and other cooking tips.

Contract Requirements for Service Providers and Contractors

The CPRA creates a new obligation requiring a business that collects a consumer's personal information to execute written contracts containing specific provisions whenever it discloses that personal information to a service provider or contractor for a business purpose.

The proposed regulations set forth several contractual requirements for persons who are to be considered service providers or contractors under the CCPA. The purpose of this regulation is to consolidate all the provisions that must be included in a service provider or contractor's contract with the business, to explain the consequence if the provisions are not included in the contract, and to clarify the duties of a service provider, contractor, and business as it relates to the contract. This allows relevant parties to use the regulation as a checklist to ensure that all the statutorily required information is included in their contracts.

Under the proposed regulations, the contract required by the CCPA for service providers and contractors must:

(A) Prohibit the service provider or contractor from selling or sharing personal information it receives from, or on behalf of, the business.

(B) Identify the specific business purpose(s) and service(s) for which the service provider or contractor is processing personal information on behalf of the business and specify that the business is disclosing the personal information to the service provider or contractor only for the limited and specified business purpose(s) set forth within the contract. **The business purpose or service shall not be described in generic terms,**

such as referencing the entire contract generally. The description shall be specific.[8] (Emphasis Added.)

(C) Prohibit the service provider or contractor from retaining, using, or disclosing the personal information received from, or on behalf of, the business for any purposes other than those specified in the contract or as otherwise permitted by the CCPA and its regulations. This section shall list the specific business purpose(s) and service(s) identified in (2) above.

(D) Prohibit the service provider or contractor from retaining, using, or disclosing the personal information received from, or on behalf of, the business for any commercial purpose other than the business purposes specified in the contract, including in the servicing of a different business, unless expressly permitted by the CCPA or these regulations.

(E) Prohibit the service provider or contractor from retaining, using, or disclosing the personal information received from, or on behalf of, the business outside the direct business relationship between the service provider or contractor and the business, unless expressly permitted by the CCPA or these regulations. For example, a service provider or contractor shall be prohibited from combining or updating personal information received from, or on behalf of, the business with personal information that it received from another source unless expressly permitted by the CCPA or these regulations.

(F) Require the service provider or contractor to comply with all applicable sections of the CCPA and its regulations, including providing the same level of privacy protection as required by businesses by, for example, cooperating with the business in responding to and complying with consumers' requests made pursuant to the CCPA, and implementing reasonable security procedures and practices appropriate to the nature of the personal information received from, or on behalf of, the business to protect the personal information from unauthorized or illegal access, destruction, use, modification, or disclosure in accordance with Civil Code § 1798.81.5.

(G) Grant the business the right to take reasonable and appropriate steps to ensure that the service provider or contractor uses the personal information that it received from, or on behalf of, the business in a manner consistent with the business's obligations under the CCPA and its regulations. Reasonable and appropriate steps may include ongoing manual reviews and automated scans of the service provider's system and regular assessments, audits, or other technical and operational testing at least once every 12 months.

[8] The reasoning for this regulation is to address observations and comments received that businesses' contracts do not clearly identify the business purpose for which the service provider is processing personal information. For example, most contracts simply state "for the specific business purpose as specified in the Agreement." This will no longer be acceptable, and the business must clearly articulate the intended business purpose or use.

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

(I) Grant the business the right, upon notice, to take reasonable and appropriate steps to stop and remediate the service provider's or contractor's unauthorized use of personal information. For example, the business may require the service provider or contractor to provide documentation that verifies that they no longer retain or use the personal information of consumers that have made a valid request to delete with the business.

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

While the proposed regulations attempt to aggregate all contract requirements from the CCPA/CPRA to have an easy reference for businesses, it appears there are missing items. For example, under the definition of "contractor," the written contract for contractors requires a certification made by the contractor that the contractor understands the contractual restrictions and will comply with them. However, this certification requirement is not mentioned in the proposed regulations. Maybe the drafters attempted to consolidate the certification requirement with the sixth item above (i.e., item F, requiring contractors or service providers to comply with the CCPA); however, further clarification is needed.

A service provider or contractor must comply with the terms of the contract required by the CCPA and the regulations. The reasoning behind this requirement is that it is necessary to make clear that a failure to comply with the required contract is a violation of the CCPA enforceable by the Agency and the Attorney General's Office.

A person who does not have a contract that complies with the above requirements is not a "service provider" or a "contractor" under the CCPA. For example, a business's disclosure of personal information to a person who does not have a contract that complies with the above requirements may be considered a sale for which the business must provide the consumer with the right to opt-out of sale/sharing.

Subcontractors of Service Providers or Contractors

A service provider or contractor that subcontracts with another person in providing services to the business for whom it is a service provider or contractor shall have a contract with the subcontractor that complies with the CCPA and its regulations. The reasoning for this regulation is to facilitate compliance with the updated definitions in the CCPA, which requires service providers and contractors who subcontract with another person in providing services to comply with the CCPA and its regulations.

Third Parties

The CPRA adds requirements on third parties who are forwarded consumer requests from a business who sold or shared personal information with them. The purpose of proposed regulations

related to third parties is to clarify what is required of third parties with regard to a consumer's CCPA requests.

Requests to Delete or Opt-Out of Sale/Sharing

A third party must comply with a consumer's request to delete or request to opt-out of sale/sharing forwarded to them from a business that provided, made available, or authorized the collection of the consumer's personal information. The third party must comply with the request in the same way a business is required to comply with the request. The third party shall no longer retain, use, or disclose the personal information unless the third party becomes a service provider or contractor that complies with the CCPA.

Requests to Limit Use and Disclosure of Sensitive Personal Information

A third party shall comply with a consumer's request to limit forwarded to them from a business that provided, made available, or authorized the collection of the consumer's sensitive personal information for purposes other than those set forth in § 7027(l) of the proposed regulations. § 7027(l) provides certain purposes for which a business may use or disclose sensitive personal information without being required to offer a right to limit. Specifically, a business that only uses or discloses sensitive personal information as listed below is not required to post a notice of right to limit:

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

(B) To detect security incidents that compromise the availability, authenticity, integrity, and confidentiality of stored or transmitted personal information, provided that the use of the consumer's personal information is reasonably necessary and proportionate for this purpose.

(C) To resist malicious, deceptive, fraudulent, or illegal actions directed at the business and to prosecute those responsible for those actions, provided that the use of the consumer's personal information is reasonably necessary and proportionate for this purpose.

(D) To ensure the physical safety of natural persons, provided that the use of the consumer's personal information is reasonably necessary and proportionate for this purpose.

(E) For short-term, transient use, including, but not limited to, nonpersonalized advertising shown as part of a consumer's current interaction with the business, provided that the personal information is not disclosed to another third party and is not used to build a profile about the consumer or otherwise alter the consumer's experience outside the current interaction with the business.

(F) To perform services on behalf of the business, 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 business.

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

The third party shall comply with the request in the same way a business is required to comply with the request. The third party shall no longer retain, use, or disclose the sensitive personal information for purposes other than those set forth above. It is important to note that the proposed regulations are a draft only and may be further revised.

Opt-Out Requests

A third party that collects personal information from a consumer online (e.g., through a first party's website) and receives an opt-out preference signal shall recognize the signal as a valid request to opt-out of sale/sharing and shall not retain, use, or disclose that personal information unless informed by the business that the consumer has consented to the sale or sharing of their personal information or the third party becomes a service provider or contractor that complies with the CCPA.

The drafters of the proposed regulations deem this regulation necessary to efficiently effectuate a consumer's request to opt-out of sale/sharing with the multiple third parties that may be collecting a consumer's personal information online. Requiring a third party who has been authorized to collect personal information from the consumer to check for and comply with an opt-out preference signal unless told otherwise prevents a third party from avoiding its obligations to comply with requests to opt-out of sale/sharing. This also benefits businesses by sharing the burden of communicating online requests to opt-out of sale/sharing and benefits consumers by ensuring that third parties tracking them online comply with their requests.

Contract Requirements for Third Parties

Similar to service providers and contractors discussed above, the proposed regulations create a new obligation requiring a business that sells or shares personal information with a third party to execute written contracts containing specific provisions.

The proposed regulations are intended to clearly set forth all the provisions that must be included in third party contract with the business and clarify the duties of the third party and the business as it relates to the contract.

With that, a business that sells or shares a consumer's personal information with a third party shall enter into an agreement with the third party that:

(A) Identifies the limited and specified purpose(s) for which the personal information is sold or disclosed. The purpose shall not be described in generic terms, such as referencing the entire contract generally. The description shall be specific.

(B) Specifies that the business is disclosing the personal information to the third party only for the limited and specified purposes set forth within the contract and requires the third party to only use it for those limited and specified purposes.

(C) Requires the third party to comply with all applicable sections of the CCPA and its regulations, including providing the same level of privacy protection as required by businesses by, for example, only collecting and using personal information for purposes an average consumer would reasonably expect or other disclosed purposes compatible with the context in which it was collected, complying with a consumer's request to opt-out of sale/sharing forwarded to it by a first party business, providing the required disclosures and implementing reasonable security procedures and practices appropriate to the nature of the personal information received from the business to protect the personal information from unauthorized or illegal access, destruction, use, modification, or disclosure in accordance with Civil Code § 1798.81.5.

(D) Grants the business the right to take reasonable and appropriate steps to ensure that the third party uses the personal information that it received from, or on behalf of the business, in a manner consistent with the business's obligations under the CCPA and its regulations.[9]

(E) Grants the business the right, upon notice, to take reasonable and appropriate steps to stop and remediate unauthorized use of personal information.[10]

(F) Requires the third party to notify the business no later than five business days after it makes a determination that it can no longer meet its obligations under the CCPA and its regulations.

A third party must comply with the terms of the contract required by the CCPA and the regulations. The reasoning behind this requirement is that it is necessary to make clear that a failure to comply with the required contract is a violation of the CCPA enforceable by the California Privacy Protection Agency and the Attorney General's Office.

A business that authorizes a third party to collect personal information from a consumer through its website either on behalf of the business or for the third party's own purposes, shall contractually require the third party to check for and comply with a consumer's opt-out preference signal unless informed by the business that the consumer has consented to the sale or sharing of their personal information. This reasoning for this is so that a consumer's election to opt-out is implemented by all persons who receive the consumer's personal information online.

A third party that does not have a contract that complies with the contract requirements discussed above may not collect, use, process, retain, sell, or share the personal information received from the business. This was added to ensure compliance with the CCPA and inform third parties of the consequences of failing to have the required contract in place.

Defenses for Service Provider, Contractor, or Third Party Violations

The CCPA, under California Civil Code § 1798.145(i) (effective as of January 1, 2023), states that a business that discloses personal information to a service provider, contractor, or third party in

[9] For example, the business may require the third party to attest to their compliance with contract requirement #3.

[10] For example, the business may require the third party to provide documentation that verifies that they no longer retain or use the personal information of consumers who have had their request to opt-out of sale/sharing forwarded to them by the first party business.

compliance with the CCPA *shall not be liable* if the service provider, contractor, or third party receiving the personal information uses it in violation of the restrictions, provided that, at the time of disclosing the personal information, the business does not have actual knowledge, or reason to believe, that the service provider, contractor, or third party intends to commit such a violation.

The proposed regulations touch on this defense. Specifically, the proposed regulations state that whether a business conducts due diligence of its service providers, contractors, or third parties factor into whether the business has reason to believe that a service provider, contractor, or third party is using personal information in violation of the CCPA. For example, depending on the circumstances, a business that never enforces the terms of the contract nor exercises its rights to audit or test the service providers, contractors, or third parties systems might not be able to rely on the defense that it did not have reason to believe that the service provider, contractor, or third party intends to use the personal information in violation of the CCPA at the time the business disclosed the personal information to the service provider, contractor, or third party.

This reasoning for this regulation is to ensure that the provisions required to be in the contract have real meaning and that businesses do not neglect their duties to ensure that personal information disclosed to service providers, contractors, or third parties is used in a lawful manner.

The proposed regulations will have a critical impact on businesses in California because if the business never enforces the terms of the contract nor exercises its rights to audit or test the service providers, contractors, or third parties systems or records may not be able to claim that it did not know or have reason to believe that the service provider, contractor, or third party intended to use the personal information in violation of the CCPA.

Financial Sector Privacy Law Exemptions to the CCPA/CPRA and its Regulations

Financial institutions do not need to comply with the above-mentioned contractual requirements if the contractual relationship is entirely covered under any of the limited exemptions for financial sector privacy laws. As mentioned above, the CPRA maintained the CCPA's limited financial sector privacy law exemptions by providing, except with respect to the CCPA/CPRA's private right of action for certain data breaches, the requirements of the CCPA/CPRA do not apply to personal information *collected, processed, sold or disclosed subject to* (i) the federal Gramm-Leach-Bliley Act ("GLBA"), as implemented by Regulation P; (ii) the California Financial Information Privacy Act ("CalFIPA"); and (iii) the federal Fair Credit Reporting Act ("FCRA").

Based on the plain reading of the statutory text, financial sector privacy law exemptions only provide an exemption to the *type of data elements* involved and not financial institutions generally. Given that these exemptions do not provide a blanket entity level exception, financial institutions may need to comply with the CPRA's extensive contract requirements with their service providers, contractors or third-parties if the data involved is not collected, processed, sold or disclosed pursuant to these financial sector privacy laws. Financial institutions should undertake a review of their contractual relationships to determine whether the data involved is subject to a financial sector privacy law exemption, and to the extent it is not, financial institutions will need to revise their contracts to conform to CPRA's requirements unless another exemption applies to the relationship.

Aside from the financial sector privacy law exemptions, the following exemptions may also apply to vendor contracts:

- Workforce and employment related personal information exemption. Currently, this exemption is set to expire on January 1, 2023.
- The vendor does not process data involving California residents. If the data involved does not pertain to California residents, the CCPA/CPRA will not apply to the contract.
- Publicly available records. If the data involved is available from publicly available records, then such data is not considered to be "personal information" for purposes of the CCPA/CPRA. Under the CPRA, "publicly available records" was revised to mean: (i) information that is lawfully made available from federal, state, or local government records; (ii) information that a business has a reasonable basis to believe is lawfully made available to the general public by the consumer or from widely distributed media; or (iii) information made available by a person to whom the consumer has disclosed the information if the consumer has not restricted the information to a specific audience.
- Deidentified or Aggregated Consumer Information. Deidentified or aggregated consumer information is excluded from the definition of "personal information" and therefore the CCPA/CPRA does not restrict businesses from collecting, using, retaining, selling, or disclosing such data. However, if the contract with the vendor deals with deidentified or aggregate consumer information, the CPRA requires such contracts to require the vendor to take reasonable measures to ensure that the information cannot be associated with a consumer or household and to publicly commit to maintain and use the information in deidentified form and not to attempt to reidentify the information, except that the business may attempt to reidentify the information solely for the purpose of determining whether its deidentification processes satisfy legal requirements.

7. Data Security and Risk Assessment Requirements

The CPRA requires businesses to implement reasonable security procedures and practices appropriate to the nature of the personal information they handle in order to protect it from unauthorized or illegal access, destruction, use, modification, or disclosure, but does not define reasonable security procedures and practices.

The CPRA also requires the implementation of regulations relating to additional requirements for businesses that process personal information in a manner presenting a significant risk to consumers' privacy or security. Such businesses are required to undergo an annual, independent cybersecurity audit and to submit an annual risk assessment to the newly created Agency. However, the CPRA does not define what constitutes processing personal information in such manner that would require businesses to comply with this requirement.

While the proposed regulations do not address the foregoing issues, it is likely that the updated/final regulations may provide more clarity for businesses on these issues.

Investigations and Enforcement

The CPRA establishes the Agency that is tasked with enforcing the CCPA. The proposed regulations set forth the mechanism for filing sworn complaints, the right for the Agency to open

complaints on the Agency's own initiative, probable cause proceedings, stipulated orders, and agency audits.

(A) Sworn Complaints Filed with the Agency. The CPRA requires that the Agency investigate possible violations. The proposed regulations implements such requirement and sets forth the requirements and mechanisms for filing sworn complaints. Sworn complaints may be filed with the Enforcement Division electronically via the Agency's website or submitted in person or by mail to the Agency at the address provided. The proposed regulations also provide the information that must be included with the sworn complaint that is necessary for the Agency to evaluate the complaint and make a determination on the appropriate response and requires that the complainant authorize the Agency to communicate with the alleged violator.

Additionally, the proposed regulations implement the requirement under the CPRA that the Agency notify the complainant in writing of the action, if any, the Agency has taken or plans to take on the sworn complaint as well as the reasons for such action or inaction.

(B) Agency Initiated Investigations. The proposed regulations provide the Agency with discretion to open a complaint against a business on its own initiative that is not the result of a sworn complaint.

(C) Probable Cause Proceedings. The CPRA allows the Agency to initiate an administrative hearing process after it determines that there is probable cause for believing a violation has occurred. The proposed regulations provide that probable cause exists when the evidence supports a reasonable belief that the CCPA has been violated. This definition only establishes the standard that must be met prior to initiating an administrative hearing but does not necessarily mean that a violation has occurred. A violation must be proven in a subsequent administrative hearing. The details about probable cause proceedings are also set forth in the proposed regulations. Among other things, the proceedings are generally closed to the public unless the alleged violator files a written request with the Agency to make the proceeding public.

(D) Stipulated Orders. Under the proposed regulations, the Head of Enforcement and the person who is the subject of the investigation may stipulate to the entry of an order before or during administrative hearing. This would allow the parties to settle matters and preserve the resources of the parties and the Administrative Law Judge.

(E) Agency Audits. The CPRA authorizes the Agency to conduct audits of businesses to ensure compliance with the CCPA. The proposed regulations set forth the Agency's criteria for selecting the subject of an audit to investigate potential violations of the CCPA which may be the result of complaints received by the Agency, self-disclosed violations, media or news reports, or any other evidence obtained by the Agency.

As noted above, the CPRA also authorizes the Agency to conduct an audit if a business processes personal information in a manner that presents a significant risk to consumers' privacy or security, which is addressed in the proposed regulations. However, it is still

unclear what constitutes processing personal information in a manner that presents a significant risk to consumers' privacy or security.

A business's failure to cooperate during an audit may result in the Agency issuing a subpoena, seeking a warrant, or otherwise exercising its power to ensure compliance with the CCPA.

As a side note, the NCUA has previously indicated that it has the sole authority to audit federal credit unions which has been used as a preemption against audits by the State Controller's Office. It remains to be seen if NCUA will extend such authority to the audits required by the Agency.

8. CPRA-Opt-Out Preference Signals

The proposed regulations address a business' handling of opt-out preference signals. Per the regulations, an opt-out preference signal is intended to "provide consumers with a simple and easy-to-use method by which consumers interacting with businesses online can automatically exercise their right to opt-out" of the sale or sharing of their personal information. A consumer will be able to utilize an opt-out preference signal to opt out of the sale and sharing of their personal information with all businesses with which they interact online without having to make an individualized request with each business.

Under the statutory requirements of the CCPA and the CPRA, businesses are generally required to include clear and conspicuous links on their homepage titled "Do not Sell or Share My Personal Information" and "Limit the Use of My Sensitive Information" that enable consumers to either opt-out of the sale and sharing of their personal information or to otherwise limit the use or disclosure of their personal information. However, if a business honors opt-out preference signals that are sent with the consumer's consent pursuant to technical specifications established by regulation, the statutory framework does not appear to require the business to also include the weblinks.

The regulations make clear that businesses are <u>required</u> to honor any opt-out preference signal that meets certain requirements as a valid consumer request to opt out of the sale or sharing of their personal information, regardless of the presence or lack thereof of opt-out links. For an opt-out preference signal to be valid, (1) the signal must be in a format commonly used and recognized by a business, such as an HTTP header field, and (2) the platform, technology, or mechanism that sends the opt-out preference signal must make clear to the consumer (whether by its configuration or by public disclosure, which does not have to be California specific) that use of the signal is intended to have the effect of opting the consumer out of the sale and sharing of their personal information.

Receipt of an opt-out preference that meets the regulatory requirements triggers a number of obligations and responsibilities on the part of the business:

(A) The signal must be treated as a valid request to opt-out of the sale or sharing of personal information collected from that browser or device, and, if known, for the specific consumer. The regulations provide the following example:

(i) Caleb visits Business N's website using a browser with an opt-out preference signal enabled. Business N collects and shares Caleb's browser identifier for cross-contextual advertising, but Business N does not know Caleb's identity because he is not logged into his account. Upon receiving the opt-out preference signal, Business N shall stop selling and sharing Caleb's browser identifier for cross-contextual advertising, but it would not be able to apply the request to opt out of the sale/sharing to Caleb's account information because the connection between Caleb's browser and Caleb's account is not known to the business.

(B) The business may not require the consumer to provide additional information beyond what is necessary to send the signal, however, it may offer the consumer the option to provide additional information that will help facilitate the opt-out request, so long as the information provided by the consumer is not used, disclosed, or retained for any other purpose. For example:

(i) Noelle has an account with Business O, an online retailer who manages consumer's privacy choices through a settings menu. Noelle's privacy settings default to allowing Business O to sell and share her personal information with the business's marketing partners. Noelle enables an opt-out preference signal on her browser and then visits Business O's website. Business O recognizes that Noelle is visiting its website because she is logged into her account. Upon receiving Noelle's opt-out preference signal, Business O shall treat the signal as a valid request to opt-out of sale/sharing and shall apply it to her device and/or browser and also to her account and any offline sale or sharing of personal information. Business O may inform Noelle that her opt-out preference signal differs from her current privacy settings and provide her with an opportunity to consent to the sale or sharing of her personal information, but it must process the request to opt-out of sale/sharing unless Noelle instructs otherwise.

(C) The business may not interpret the absence of an opt-out preference signal after the consumer previously sent an opt-out preference signal as consent to opt-in to the sale or sharing of personal information:

(i) Noelle revisits Business O's website at a later time using a different browser that does not have the opt-out preference signal enabled. Business O knows that it is Noelle because she is logged into her account. Business O shall not interpret the absence of the opt-out preference signal as consent to opt-in to the sale of personal information.

(D) If the opt-out preference signal conflicts with the business-specific privacy setting that allows the business to sell or share their personal information, the business must process the opt-out preference signal, however, it may notify the consumer of the conflict and provide the consumer with the opportunity to consent to the sale or sharing of their information.

(E) If the opt-out preference signal conflicts with the consumer's participation in a business's financial incentive program that requires the consumer to consent to the sale or sharing of personal information, the business must notify the consumer of this fact before processing the opt-out preference signal and ask the consumer to confirm that they intend to withdraw from the incentive program. Note that this differs from those situations referenced above where there is simply a conflict between the consumer's general opt-out preference signal and their business specific setting, where the business must proceed with processing the opt-out preference signal and permit the consumer the opportunity to opt-back in. The regulations provide an example of how the process works in the context of a financial incentive program:

(i) Ramona participates in Business P's financial incentive program where she receives coupons in exchange for allowing the business to pseudonymously track and share her online browsing habits to marketing partners. Ramona enables an opt-out preference signal on her browser and then visits Business P's website. Business P knows that it is Ramona through a cookie that has been placed on her browser, but also detects the opt-out preference signal. Business P may ignore the opt-out preference signal, but must notify Ramona that her opt-out preference signal conflicts with her participation in the financial incentive program and ask whether she intends to withdraw from the financial incentive program. If Ramona does not affirm her intent to withdraw, Business P may ignore the opt-out preference signal and place Ramona on a whitelist so that Business P does not have to notify Ramona of the conflict again.

(F) The business should display whether it has honored the consumer's opt-out preference signal through a toggle or radio button, or text that indicates the signal has been honored, such as "Opt-Out Preference Signal Honored."

"Frictionless" Processing

As mentioned, the regulations make clear that a business must process valid opt-out preference signals. The regulations go on to provide that if the business processes opt-out preference signals in a "frictionless" manner, it may, but is not required to, provide the "Do not Sell or Share My Personal Information" and "Limit the Use of My Sensitive Information." Frictionless processing of an opt-out preference signal means that the business does not:

(A) Charge a fee or require any valuable consideration if the consumer uses an opt-out preference signal.

(B) Change the consumer's experience with the product or service offered by the business (e.g., product or service functionality is the same for a consumer that does or does not use an opt-out preference signal).

(C) Display a notification, pop-up, text, graphic, animation, sound, video, or any interstitial content in response to the opt-out preference signal. This does not prohibit the businesses from displaying that it has honored the opt-out preference signal or a link to

a settings page or menu that enables the consumer to consent to the business ignoring the opt-out preference signal.

We note that the regulations would allow businesses to process opt-out preference signals in a "non-frictionless" manner, in which case the business would be required to post the "Do not Sell or Share My Personal Information" and "Limit the Use of My Sensitive Information" links.

If the business processes the opt-out preference signals in a frictionless manner, it is not required to post the "Do not Sell or Share My Personal Information" and "Limit the Use of My Sensitive Information" links so long as it also:

(A) Includes in its privacy policy (1) a description of the consumer's right to opt-out of the sale or sharing of their personal information, (2) a statement that the business processes opt-out preference signals in a frictionless manner, (3) information on how consumers can implement opt-out preference signals for the business to process in a frictionless manner, and 4) instructions for any other method by which the consumer may submit a request to opt-out of sale/sharing.

(B) Allows the opt-out preference signal to fully effectuate the consumer's request to opt-out of sale/sharing. The regulations provide examples for what this means practically:

(i) Business Q collects consumers' online browsing history and shares it with third parties for cross-contextual advertising purposes. Business Q also sells consumers' personal information offline to marketing partners. Business Q cannot fall within the exception set forth in Civil Code § 1798.135, subdivision (b)(1) because a consumer's opt-out preference signal would only apply to Business Q's online sharing of personal information about the consumer's browser or device; the consumer's opt-out preference signal would not apply to Business Q's offline selling of the consumer's information because Business Q could not apply it to the offline selling without additional information provided by the consumer, i.e., the logging into an account.

(ii) Business R only sells and shares personal information online for cross-contextual advertising purposes. Business R may use the exception set forth in Civil Code § 1798.135, subdivision (b)(1) and not post the "Do Not Sell or Share My Personal Information" link because a consumer using an opt-out preference signal would fully effectuate their right to opt-out of the sale or sharing of their personal information.

For now, we can expect that updates to CCPA/CPRA privacy policies and practices will be required in response to these Regulations pertaining to opt-out signal preferences. Hopefully, as the regulations are finalized, the Agency will provide more detail and examples for what constitutes an opt-out preference signal so that businesses subject to the CCPA and CPRA can be better prepared for their compliance obligations.

B. Regulatory Compliance Impacting California Lending

We are often asked about what examiners may be focusing on in coming examinations, as well as what is coming on the legal horizon. Forecasting in any field is notoriously difficult, but in the inflationary and rising rate environment we are coming into, we believe there are a number of areas where financial institutions can review and help mitigate risk in this environment. In this section, we discuss areas where financial institutions may be able to focus audit, compliance, and operational time in order to mitigate legal and compliance risk in a rising rate environment, and point to areas in which financial institutions can get "tripped up" in rapidly changing rate environments.

1. Legal and Regulatory Issues in a Rising Rate Environment

General Supervisory Priorities

Naturally, regulatory guidance is a place to start. While the NCUA's Supervisory Priorities, found in Letter to Credit Unions 22-CU-02, the OCC's Supervision Operating Plan, and the CFPB's Supervisory Highlights provide significant insight, they are in part backwards-looking. They were also published before the Federal Reserve's recent aggressive interest rate increases. In many ways, these published supervisory priorities largely correspond with those of the last few years. Highlights which remain consistent include: cybersecurity; credit risk management; consumer compliance; payment systems; CECL implementation; and BSA/AML compliance. Of these, recession may impact both credit risk and the analysis of portfolios under various CECL methodologies.

The OCC and NCUA each note interest rates, but largely as it relates to LIBOR's sunset and the glut of deposits resulting from pandemic conditions. The current rate environment and inflation have not been in their supervisory picture, but will doubtless live large in examinations.

An interesting note at the outset of the OCC's plan is that examiners are to guard against complacency. This is an important note for all Boards and management teams. The OCC states:

> "Examiners should focus on strategic and operational planning to ensure banks maintain stable financial positions, especially regarding capital, the allowances for credit losses, management of net interest margins, and earnings. Examiners should ensure banks remain vigilant when considering growth and new profit opportunities and will assess management's and the board's understanding of the impact of new activities on the bank's financial performance, strategic planning process, and risk profile."

While the OCC focuses on looking for hidden risks and impacts, the opposite understanding of complacency may be considered when applying to credit union operations. The world continues to change, and we can see the NCUA beginning to shift gears away from legacy thinking with its proposed Succession Planning rule. Credit unions will, in the coming years, be challenged to understand and act on their mission and move their operations forward. We believe this often involves considering strategic plan, FOM, leadership, and incentives for service to help promote

health and keep complacency at bay. FinTech and NeoBank competition is here, and understanding identity, market, and role will be vital to survival and success of financial institutions.

Impacts in Lending

Lending areas carry a number of key compliance and legal risks that can be impacted in a rising rate environment, and which can result in costly mistakes.

(A) Rate lock commitments: Particularly in real estate and commercial loans, rate lock commitments can be important selling points for borrowers. These are contractual commitments, and can greatly impact whether borrowers can afford purchases. However, particularly with commercial loans, the time between a "Letter of Intent" ("LOI") and loan documentation can be significant. Accordingly, appropriate language protecting an lender's interests is vital.

Among other things, and particularly in the current environment, LOIs should:

- Have shorter termination periods, and provide the lender with the ability to terminate its commitment or rate in the event of adverse macroeconomic changes.
- Have short rate lock periods, particularly for fixed rate loans.
- Include all conditions precedent necessary to recognize the value of the transaction—for example, if a lender is relying on participation arrangements on a commercial real estate loan to be able to make the loan, obtaining participant commitments may be named as a condition precedent to closing.

Other types of commitments come in conditional approval letters—letters issued after underwriting is done and management approves the underwriting. Such conditional approval letters should have short closing periods for the borrower to meet all conditions precedent to close. Waiting weeks or months between final underwriting approval and closing for a borrower to be able to satisfy the closing conditions for purchase can prejudice the lender's value in the loan, and especially its ability to sell the loan or participation interests.

Breaches of LOIs can result in lender liability, but breach of a conditional approval letter can carry much more significant consequences—at the phase of a conditional approval letter, the borrower is in the final stage of a purchase, and it can be clearly shown that economic damages (both earnest money deposits and other damages) resulting from a pull-out were caused by the lender's breach.

The best protection against lender liability without being "stuck" in stale deals is careful drafting of conditional approval letters to take into account changing market conditions and any other business realities applicable to the transaction.

This leads to an important conclusion: for LOIs and conditional approval letters to protect a lender in this rapidly changing environment, lending departments, finance, secondary markets, and other asset-liability management teams must all be actively

discussing dependencies around the institution's pipeline and its balance sheet management strategies. Without discussion with and input from other stakeholders, lending teams' "boots on the ground" will not be able to adequately capture protections for the lender's interest.

(B) Variable rate adjustments: Variable rate loans significantly improve an institution's interest rate risk during a low-rate period. Lenders holding a significant book of variable loans will fare well in the current environment. However, regulatory elements of the documentation and operation of variable rate loans can lead to mistakes. Application of TILA/Regulation Z and state contract law can result in both "actual damages" and statutory penalties, and regulators who identify issues with rate adjustments or documentation will generally require institutions to engage in error correction processes (even if TILA safeharbor timeframes have passed).

Accordingly, a summary of areas to review to ensure compliance includes:

- Review contracts for floors and caps; make sure your systems reflect both. Missing a floor is lost money; missing a cap will result in refunds of interest.
- Review contracts for when rates adjust and what the maximum rate adjustment in any single step is. For example, consider a note which provides that the rate adjusts at the 5th anniversary of origination and each anniversary thereafter (e.g., a 5/1 ARM), that rates will be rounded up to the next .25, and that rates cannot increase by more than 150 bps in a single adjustment. Mortgages originated in 2017 were at rates around 3.15%, while the average 5/1 ARM in June 2022 was closer to 4.15%. Increases in July may well push the Prime rate further up. Our example of a 150 bp maximum increase might be safe today, but a note with a 100 bp maximum increase might be hitting its maximum.
- Review ARM rate adjustment disclosures under 12 CFR 1026.20(d) and (c). These adjustment notices require very specific verbiage and very specific timing. Unfortunately, some loan servicing software does not, by default, accurately produce these disclosures.

Impacts for Loan Purchases

Loan production over the past several years has been a situation with "haves" and "have nots"—significant production has been occurring for key institutions with key relationships and channels. But for consumer loan production, many financial institutions, particularly many credit unions, have seen slow demand, and at the same time experienced record deposit growth and continued cost inflation. In this context, many credit unions have been purchasing loans from the credit unions that have been fortunate enough to have FinTech and other relationships (and corresponding fields of membership) to have excess loan demand. Such purchases for FCUs are permitted through the Eligible Obligations and Participation rules, which allow purchase from an originating credit union, but also under a 2015 legal opinion allows a flexible interpretation of who the "originator" is in indirect lending situations. But state-chartered credit unions must also follow state law governing such acquisitions, which may differ from federal rules.

Close compliance with these rules is important, as if a credit union purchases a loan it is not permitted to buy, the applicable regulators may require the buyer to divest of the asset. While loan pools remain profitable, older pools with lower rates are not necessarily marketable. Loans with lower rates purchased over the last couple years may only be saleable at a discount. This creates significant risk if memberization and origination issues are not carefully attended to.

In California, Financial Code 14959 governs a California credit union's ability to purchase loans. The statute reads (in pertinent part):

> "(a) A credit union may do either or both of the following:
>
> (1) Purchase, in whole or in part, from any source, loans made to its members.
>
> (2) Sell, in whole or in part, to any source, loans made to its members.
>
> (b) A credit union may purchase, in whole or in part, either or both of the following:
>
> (1) A loan originated by another credit union, which is made to a member of the originating credit union even though the member is not also a member of the credit union purchasing the loan.
>
> (2) A loan from any source, if the purchase will facilitate the purchasing credit union's packaging of a pool of those loans to be sold or pledged on the secondary market."

This statute changed in 2019, with the prior versions not permitting whole loan purchases.

As noted in the California Senate Floor analysis, the intent of the changes to § 14959 in 2018 (effective January 1, 2019) was to conform California law to federal law:

> "Authority to Purchase, Sell, or Pledge Whole Loans (federal conformity). Existing law limits state-chartered credit unions to purchasing parts of loans; it does not permit the purchase of whole loans. Federally-chartered credit unions are authorized to purchase, in whole or in part, within the limitations of their board of directors' written purchase policies, eligible obligations of their members, eligible obligations of a liquidating credit union's members, student loans, and real-estate secured loans. Federally-chartered credit unions are also authorized to sell, service, or pledge those obligations (NCUA Rule 701.23). This bill provides the same authority to state-chartered credit unions." [emphasis added]

The Assembly analysis agrees with and repeats this reasoning. Because of this history, one might expect that parity with FCUs would be expected, including the flexibility about "origination" in indirect lending.

Despite this, there is a rising trend of interpretation within the DFPI of Financial Code 14959 for California credit unions purchasing participations and whole loans. The DFPI is taking a close reading of the language of 14959 such that "originate" means it cannot have come first through an

indirect channel—it has to be originally on loan documents with the credit union's name on them and underwriting by the credit union.

California credit unions should exercise caution when purchasing loan pools or participations, particularly where the selling credit union partners with FinTech loan sources. Credit unions around the country should be aware when selling that credit union purchasers in different states may have different requirements, and the stability of a sale and partnership may depend on a close reading of the statutes and rules in that particular jurisdiction.

Deposits and Overdraft

At the same time as anticipation of rising rates have begun to assist with core interest income and net interest margins, trends to move away from overdraft fees began to gain traction. Indeed, earlier this year, some large banks made headlines by eliminating overdraft fees. This will naturally create pressures for smaller institutions, both by removing a degree of "regulatory cover" and by making checking accounts with overdraft fees less competitive. We see these market moves by large banks as both a response to political pressure and an "early adopter" move to maintain market share while they have competitive advantages of scale.

Accordingly, while overdraft and similar fees are not directly linked to interest rates, we believe the ability of institutions to shift away from certain sources of non-interest income will be dependent on increased interest margin. As rates rise, we believe there will be more political and regulatory will to crack down on overdraft and similar fees. Financial institutions should be prepared, and should be making their plans on how they might move away from overdraft income (as a source of income and as a product design).

Contracts

Everything costs more, it seems. Vendors will universally be looking at their margins and determining how much (not whether) rates will need to increase. Our office generally attempts to negotiate caps on such rate increases, whether tying to a fixed cap, or tying to CPI or a similar index. Without those caps, vendor contracts often permit open-ended adjustments. Financial institutions beginning to plan for budgets should be looking at key relationships to determine what the increased cost of vendor assistance will be. In contract negotiations, caps on rate increases will be necessary (to the extent that the train hasn't left the station already!).

2. CFPB Supervisory Highlights Focus On Gap Refunds and UDAAP Claims

As part of its recent supervisory highlights bulletins focusing on unfair, deceptive, or abusive acts or practices (UDAAPs) by auto servicers, the CFPB focused on issues arising from purchases of guaranteed asset protection (GAP) products. Specifically, the CFPB found that servicers engaged in unfair practices by failing to request refunds from the third-party administrators for "unearned" fees related to GAP products and failing to apply the applicable refunds to the accounts after repossession and cancellation of the contracts.

When purchasing contracts for vehicles that were sold in conjunction with a GAP product, lenders need to be aware of the legal framework regarding responsibility for returning "unearned" GAP premiums (i.e., the portion of the fees that would have covered a period during which the borrower

no longer owns the vehicle or is otherwise no longer in need of the product). Contracts between the dealer and the purchasing indirect lender should, in the absence of an applicable legal framework dictating responsibility for refunds, be very clear about who has the responsibility to provide consumers with information regarding obtaining refunds and who is responsible for assisting consumers with obtaining such refunds. To the extent that agreements leave the division of responsibilities an open question or impose the responsibility on lenders, the failure of a lender to proactively assist consumers with obtaining a refund of unearned fees could leave it vulnerable to UDAAP claims. However, lenders would also be well served tracking those contracts where a GAP refund may be owed to a borrower, and reaching out to the dealer to initiate a refund of GAP premium refunds.

C. Employment Updates

1. Naranjo v. Spectrum Security Services, Inc.

On May 23, 2022, the California Supreme Court, in *Naranjo v. Spectrum Security Services, Inc.*,[11] held that missed meal and rest break premium pay constitutes "wages" under California law. This long-awaited decision is an unfortunate blow to employers as California reiterates its employee-friendly stance; it will significantly impact on employers in California and increase potential liability for meal and rest break violations.

Background Facts and Procedural History

Gustavo Naranjo ("Plaintiff") was employed by Spectrum Security Services, Inc. ("Defendant"). Plaintiff was suspended and later fired by Defendant after leaving his post as a guard to take a meal break, in violation of Defendant's policy that required some employees to remain on duty during all meal breaks.

Soon thereafter, Plaintiff filed a class action lawsuit alleging that Defendant had violated California law (i.e., meal break requirements).[12] Specifically, Plaintiff sought an additional hour of pay for missed meal breaks for each day Defendant failed to provide a compliant meal break. The additional hour of pay for missed meal breaks is commonly referred to as "premium pay." In addition to the premium pay, Plaintiff alleged that Defendant was required to report the premium pay on employees' wage statements and timely provide the pay to employees upon their discharge or resignation.

The trial court initially granted summary judgment in favor of Defendant, but the California Court of Appeal reversed. On remand, the trial court certified a class for the meal break and related timely payment and wage statement claims and then held a trial in stages.

During the trial, the trial court considered an exception to the meal break requirement that allows for " 'on duty' "meal periods if "the nature of the work prevents an employee from being relieved of all duty," but only when "by written agreement between the parties an on-the-job paid meal period is agreed to."[13]

[11] Naranjo v. Spectrum Security Services, Inc., 13 Cal. 5th 93 (2022)
[12] Cal. Labor Code § 226.7(c); IWC Wage Order No. 4-2001
[13] IWC Wage Order No. 4-2001 § 11(A)

The trial court agreed that Defendant did not have a valid written on-duty meal break agreement. Thus, the trial court ruled in favor of Plaintiff on the meal break violations during the time that Defendant did not have a written agreement as required by the IWC Wage Orders. Ultimately, the trial court entered judgment for the Plaintiff class on the meal break and wage statement claims.

The parties appealed the decision. The California Court of Appeal affirmed the trial court holding in part and reversed in part. In relevant part, the Court of Appeal affirmed the trial court's determination that Defendant violated the meal break requirements during the period without a written agreement; but reversed the trial court's holding that a failure to pay meal break premiums could support claims under the wage statement and timely payment statutes.

From there, the California Supreme Court agreed to take the case.

California Supreme Court Decision

In its review, the California Supreme Court stated that the primary questions, in this case, concern the relationship between the premium pay requirement and the provisions of the Labor Code governing the reporting of wages and timely payment of wages upon discharge or resignation.
In its review, the Supreme Court considered these issues:

(A) When an employer unlawfully denies an employee a meal or rest period and thus becomes obligated to pay premium pay, can the employer be held liable under Labor Code § 203 (regarding waiting time penalties) if it fails to pay any premium pay within statutorily mandated deadlines?

(B) And can the employer be held liable under Labor Code § 226 (regarding wage statements) if it fails to report that premium pay on a statutorily required wage statement?

Waiting Time Penalties

When an employment relationship comes to an end, the Labor Code requires employers to promptly pay any unpaid wages to the departing employee. With limited exceptions, final unpaid wages, including unused accrued vacation time, are immediately due at the time of their employment termination to any employee who either:

- Is involuntarily terminated by their employer.
- Resigns with at least 72-hours' notice of their intent to resign, when they do not have a written employment contract for a definite period.

To enforce these deadlines, Labor Code § 203 has penalties for employers who willfully fail to pay the full amounts due. Absent timely payment of "any wages of an employee who is discharged or who quits, the wages of the employee shall continue as a penalty from the due date thereof at the same rate until paid or until an action therefor is commenced; but the wages shall not continue for more than 30 days." The foregoing penalties regarding delays in end of employment wages are commonly referred to as "waiting time penalties."

As noted, the trial court agreed with Plaintiff that Defendant owed premium pay and that untimely payments could trigger penalties but found none owed because Defendant's delay was not willful.

Interestingly, the Court of Appeal affirmed the trial court's holding, but on very different grounds; it concluded that even a willful failure to pay amounts owed under § 226.7 (i.e., premium pay) could never trigger waiting time penalties under § 203. The Court of Appeal reasoned that premium pay is "unambiguously" beyond the reach of the wages definition because it is a legal remedy, not payment for labor; the premium pay is due to employees not for work they performed but as a sanction on account of the employer's violation regarding meal breaks.

The California Supreme Court held that the Court of Appeals interpretation was wrong. Specifically, the Supreme Court noted that the Court of Appeal "was correct that premium pay is a statutory remedy for a legal violation. But the court's further conclusion that premium pay cannot constitute wages rests on a false dichotomy: that a payment must be either a legal remedy or wages. For these purposes, § 226.7 is both."

The Supreme Court reasoned that the premium pay due for the meal break violations is designed to compensate employees for hardships that employees should not be made to suffer. But when those hardships include rendering work, the pay owed can equally be viewed as wages.

Ultimately, the Supreme Court ruled that the missed-break premium pay serves as a remedy for a legal violation and does not change the fact that the premium pay also compensates for labor performed under conditions of hardship. One need not exclude the other.

Thus, missed-break premium pay constitutes wages for purposes of Labor Code § 203, and thus, waiting time penalties are available under that statute if the premium pay is not timely paid.

Wage Statements

Next, the Supreme Court considered the wage statement issue. The wage statement statute requires that an employer report both "gross wages earned" and "net wages earned." To enforce the foregoing requirement, the Labor Code provides statutory penalties for the "knowing and intentional failure by an employer to comply with [§ 226]. Specifically, an employee is deemed to suffer injury (for purposes of § 226(e)) if the employer fails to provide a wage statement or fails to provide an accurate and complete statement and the employee cannot promptly and easily determine from the wage statement certain pieces of information.

However, the Labor Code clarifies that a "knowing and intentional failure" does not include an isolated and unintentional payroll error due to a clerical or inadvertent mistake. In reviewing for compliance, relevant factors include whether the employer, prior to an alleged violation, had adopted and is in compliance with a set of policies, procedures, and practices that fully comply with this section.

As the Supreme Court determined that the premium pay constitutes wages in California, this analysis was much more concise and focused on the Defendant's arguments (by which the Supreme Court was not persuaded).

For example, Defendant argued that Labor Code § 226 lists many categories of information that must be reported but contains no separate requirement that missed-break premium pay be reported.

The Supreme Court found this argument "not meaningful" as it considered the language of § 226 and stated, while true, § 226 does not contain other provisions expressly calling out any other specific sorts of pay, such as overtime pay; however, such pay must still be reported.[14]

Thus, the Supreme Court held that an employer's obligation under Labor Code § 226 to report wages earned includes an obligation to report premium pay for missed breaks. The ramification of this ruling is that the failure to report premium pay for missed breaks can result in statutory penalties.

What Does This Mean for California Employers?

This Supreme Court ruling reinforces California's pro-employee stance and will have major implications for California employers. We can expect an uptick of cases resulting from this ruling (especially with class action lawsuits).

Thus, California employers are strongly encouraged to review and audit meal and rest break policies and practices, wage statements reporting, and final pay practices to ensure it is compliant with California law as this ruling (i.e., classifying missed-break premium pay as wages) opens the door for waiting time penalties (if the premium pay is not timely paid); and creates an obligation for employers to report premium pay for missed breaks in required wages statements (and the failure to report premium pay properly can result in statutory penalties).

2. The Employer Win Thanks to SCOTUS

Introduction

On June 15, 2022, the United States Supreme Court entered a ruling on *Viking Cruises, Inc. v. Moriana*. In *Viking*, the Court addressed whether California's application of the state's Private Attorneys General Act ("PAGA") violated or conflicted with the Federal Arbitration Act ("FAA"). The Court concluded that while PAGA, on its face, did not conflict with the FAA, the application of PAGA pursuant to the California Supreme Court's decision in *Iskanian v. CLS Transp. Los Angeles, LLC,* does create a conflict with the FAA. Based on its reasoning, the Court held that the FAA preempts PAGA insofar as the *Iskanian* decision prohibits companies from enforcing arbitration clauses in employment contracts. The *Viking* decision seems to provide California employers with some relief from the enormity of PAGA claims. The Court's decision, however, does leave the door open for the California legislature to amend the state law to close what may appear to be a "loophole" in the enforcement of PAGA actions. This article will discuss the *Viking* decision and the immediate ramifications it caused in labor and employment in California.

Background – PAGA

The California Private Attorneys General Act became law in 2004 with the purpose of encouraging enforcement of California labor law protections. PAGA permits employees to file a lawsuit against the employer for Labor Code violations on behalf of themselves and on behalf of other aggrieved employees. Given an employee's option to sue on behalf of other aggrieved employees, PAGA claims have resulted in large judgments against employers. Settlements have ranged from $10,000 to over $25 million. The number of violations, size of the workforce, etc. determine how large a settlement against an employer will be. Only 25 percent of the award is paid to the aggrieved

[14] General Atomics v. Superior Court 64 Cal. App. 5th 987, 991 (2021)

employees while the bulk of the award (75%) is paid to the state. In short, a PAGA claim can be an employer's worst nightmare.

In pertinent part, PAGA created an option for employees to circumvent arbitration agreements. While employees may sign an agreement to arbitrate labor disputes, PAGA allows for an employee to file suit against the employer, bypassing any requirements to arbitrate, by filing on behalf of other aggrieved employees. In the *Iskanian* case, the California Supreme Court's decision set two relevant precedents that the U.S. Supreme Court analyzed in *Viking*: (1) As a matter of public policy, the state courts invalidate and decline to enforce arbitration agreements that waive the right of an employee to bring "representative" PAGA claims; and (2) PAGA claims essentially could not be resolved on an individual basis because PAGA claims are intended to address all Labor Code violations of the employer committed against its employees. Under the *Iskanian* rulings, employers had no way to enforce an arbitration agreement for labor disputes because waiving claims in the capacity as representative were invalid and PAGA claims are not individual in nature so an individual could not be forced to arbitrate. Essentially, the Court in *Iskanian* made individual grievances indivisible from representative claims based on the grievances of other employees. This is where the U.S. Supreme Court focused in the *Viking* case. It examined whether the FAA preempts PAGA and, thereby, renders arbitration agreements valid with PAGA claims.

The Viking Decision Explained

Angie Moriana ("Moriana") was a sales representative for Viking River Cruises, Inc. ("Viking") and, when hired, she signed an agreement under which she agreed to arbitrate any labor disputes with Viking. The agreement contained a waiver of Moriana's right to file a class action, collective action, or PAGA representative action. The agreement also contained a severability clause, which provides that, in the event that any portion of the waiver is invalidated, the remaining portion of the waiver would be enforced in arbitration. After Moriana ended her employment with Viking, she subsequently filed a PAGA action on behalf of herself and other aggrieved employees in California court. Viking requested the court order Moriana's individual claim be handled in arbitration pursuant to her arbitration agreement with Viking. The court denied Viking's request based on the *Iskanian* rulings: the waiver of PAGA representative action is invalid; and Moriana's individual claims are indivisible from the representative claims. Viking appealed to the California Court of Appeal and subsequently to the California Supreme Court. Both courts affirmed[15] the lower court's denial of Viking's request based on the *Iskanian* rulings. The U.S. Supreme Court granted certiorari and addressed whether the FAA is violated by the *Iskanian* application of PAGA.

The U.S. Supreme Court reviewed both parts of the *Iskanian* decision and concluded that only the second part is preempted by the FAA. The Court concluded that the FAA did not preempt PAGA from prohibiting waivers of PAGA representative actions. Hence, California is free to require employers to litigate representative claims and the waiver of such in Moriana's arbitration agreement with Viking would be invalid and unenforceable. However, the Court did take issue with PAGA holding individual claims and representative claims are indivisible. The Court reasoned that "States cannot coerce individuals into forgoing arbitration by taking the individualized and informal procedures characteristic of traditional arbitration off the table." Accordingly, a conflict was found between the *Iskanian* application of PAGA and the intention of the FAA, which promotes the use of alternative dispute resolution. The Court found that *Iskanian*

[15] The California Court of Appeals reviewed and affirmed. The California Supreme Court declined to review.

effectively forced employers to litigate individual PAGA claims and rendered arbitration agreements ineffective. The Court quoted language from an earlier SCOTUS opinion in *Kindred Nursing Centers L.P. v. Clark*, asserting that the FAA preempts any state rule discriminating on its face against arbitration-for example, a law prohibiting outright the arbitration of a particular claim. The Court concluded that the *Iskanian* application of PAGA does that and the FAA preempts it. As a result, the arbitration agreement for Moriana's individual claim was enforced and Moriana's representative claims were dismissed on the grounds that she now lack standing without the individual claim.

The Impact of Viking

The *Viking* decision presents (for now) a victory for California employers as it permits employers to enforce arbitration agreements requiring employees to arbitrate their individual claims, including their individual PAGA claims, and in turn, preclude the employee from suing on behalf of other aggrieved employees. While California employers had been waiting and hoping for the U.S. Supreme Court's decision, the benefits of the *Viking* decision may be short lived as the plaintiffs' bar, as well as the California legislature have promised to challenge the decision. Indeed, in her concerning opinion, Justice Sotomayor essentially laid out the legal path for California to "fix" the standing element that was key to the Viking decision. In addition, in late July, the California Supreme Court agreed to review another case involving PAGA claims against Uber. The California Supreme Court's ultimate decision in the Uber case may render the key benefit in the *Viking* case useless. The California Supreme Court's decision of the Uber case (*Adolph v. Uber Technologies, Inc.*) is likely months away and it appears that a California legislative "fix" to PAGA may be pushed to 2023. In the meantime, California employers may still want to consider implementing arbitration agreements with employees or revising existing arbitration agreements. Employers should consult with their legal counsel on such issues as there are many other facets of arbitration agreements, including the still in place injunction on AB51. Stay tuned!

D. Litigation Updates

1. Recent Class Action Litigation Arising From Zelle

There has been a recent rise in class action lawsuits involving Zelle services being offered by financial institutions, wherein class representatives are alleging, among other causes of action, violations of the Electronic Fund Transfer Act ("EFTA") and its implementing regulation, Regulation E. Of note, Bank of America, Wells Fargo, and Navy Federal Credit Union were all recently sued by customers and members who claimed that these financial institutions failed to reimburse class members for timely reported fraudulent losses incurred when using their respective financial institution's Zelle money transfer service. [16]

[16] *See Mohammad Al-Ramahi v. Bank of America, N.A.*, filed in the Northern District of California, Case No. 22-cv-03118 (May 27, 2022); *Luke Hartsock v. Wells Fargo & Company, N.A., et al*., filed in the Western District of Washington, Case No. 22-cv-200759 (June 1, 2022); *Jessica Stock v. Wells Fargo & Company, N.A., et al*., filed in the Central District of California, Case No. 22-cv-00763 (April 5, 2022); and *Jacqueline Wilkins v. Navy Federal Credit Union*, removed to the United States District Court, District of New Jersey, Case No. 22-cv-02916 (May 18, 2022).

Furthermore, the class action representatives in the above-referenced lawsuits alleged that Zelle and the defendant financial institutions misrepresented the Zelle services by misinforming customers/members that unauthorized Zelle transactions would not be covered by the respective financial institution's fraud policies while simultaneously marketing Zelle as a fast, safe, and secure way to send money. The lawsuits also go on to mention that the Zelle and the defendant financial institutions were aware of widespread fraud on Zelle but did nothing to help consumers get their money back and also, did not warn consumers of the risks of being scammed while using Zelle.

Importantly, the transactions at issue in the above lawsuits technically do not appear to be covered by Regulation E protections because the consumer/victim was the person initiating the transactions at issue, to fraudsters. As such, the transaction was not an "Unauthorized EFT" because it was not "initiated by a person other than the consumer", as required under Regulation E. These lawsuits indicate that, even if a financial institution is not subject to Regulation E's requirements, there is still the risk that a financial institution may be sued in a class action for fraudulent transactions initiated by the actual account holder.

Although the aforementioned class action lawsuits are currently working their way through the judicial system, they serve as good reminders that financial institutions should review and ensure that their fraud policies and consumer-facing documents are in line with current regulations and laws, especially with the increasing prevalence of Person-to-Person ("P2P") services such as Zelle. In fact, the application of P2P services to the EFTA/Regulation E has been a recent topic of discussion for regulatory agencies. In this regard, the CFPB issued guidance on unauthorized Electronic Funds Transfers ("EFTs"), which indicated that P2P payments are EFTs (including transactions made with Zelle) and trigger error resolution obligations under the EFTA/Regulation E that protect consumers from situations where they are fraudulently induced and requested by a third party to provide their account information that result in authorized debits from their accounts.

Please also note that there are special rules found in Regulation E that where a non-account-holding financial institution is considered an EFT service provider, as may be the case with Zelle, the corresponding account-holding financial institution may have more limited error resolution responsibilities. However, these special rules regarding limited error resolution responsibilities under Regulation E will not apply when there is an agreement between the non-account-holding financial institution (the non-bank P2P payment provider) and the account-holding financial institution (the consumer's depository institution). If there is no such agreement in place, the special rules would apply as follows: the account-holding financial institution need not comply with the requirements of the EFTA concerning EFTs initiated through the EFT service provider, including the tiered limits on a consumer's liability, except, the account-holding financial institution would need to: (1) provide a periodic statement that describes each EFT initiated by the consumer with the access device issued by the EFT service provider; and (2) upon request, provide information or copies of documents needed by the EFT service provider to investigate errors or to furnish copies of documents to the consumer. The account-holding financial institution must also honor debits to the account in accordance with Regulation E § 1005.11(d)(2)(ii).

With that, Zelle transactions are considered EFTs governed by the EFTA/Regulation E and as such, consumers are generally entitled to the error resolution protections provided for under the

EFTA/Regulation E. As noted above, there are special circumstances, that if met, will allow certain financial institutions to have more limited EFTA/Regulation E error resolution responsibilities; however, such circumstances are narrow. As a result, and since it appears that more and more fraudsters are taking advantage of one of the major benefits of P2P services, the immediacy of sending money, financial institutions should closely monitor such transactions and ensure that they are timely and appropriately responding to unauthorized EFT claims, including those perpetrated through fraud.

Based on the foregoing and given the increase in class action lawsuits related to Zelle, financial institutions should consider reviewing their consumer-facing documents and EFTA/Regulation E policies and procedures regarding fraudulent P2P transactions to ensure compliance with current laws and regulations, as well as addressing the class action litigation risk related to fraudulent transactions that are not subject to EFTA/Regulation E protections for consumers. Of course, the experts at SW&M can assist in this regard.

2. Bank of America – Garnishment Case

The CFPB recently finalized an enforcement action against Bank of America in response to Bank of America's processing of out of state garnishment orders affecting bank accounts.

As you are aware, creditors often seek garnishment orders, such as bank account levies, that allow them to collect funds from debtors. Garnishments often come from state or federal agencies, such as child support or taxing authorities. Other times, garnishments are issued by courts in which a money judgment has been issued against a person or entity. For example, in California, after receiving a civil judgment in their favor, a judgment creditor may ask the court to issue a levy against the judgment debtor's bank accounts to assist the creditor in collecting their judgment. Because this is a court order, it is generally a requirement that the court have jurisdiction over the person holding the property (in the case of a bank account levy, the bank), and the property (the bank account itself), in order for the garnishment to be enforceable.

It is also the case that many states' laws provide exceptions to garnishments that must be applied before the creditor may collect their judgment from the debtor. For example, in California, the California Code of Civil Procedure provides many exemptions to a levy, including California Code of Civil Procedure § 704.080 which exempts certain funds in a deposit account where state public benefit payments or social security payments are directly deposited by the government.

Specifically, § 704.080(b) provides in part:

> "(b) A deposit account is exempt without making a claim in the following amount:
>
> (1) One thousand seven hundred fifty dollars ($1,750) where one depositor is the designated payee of the directly deposited public benefits payments.
>
> (2) Three thousand five hundred dollars ($3,500) where one depositor is the designated payee of directly deposited social security payments …"

These funds are exempt "without making a claim," which means that it is the responsibility of the financial institution that holds the deposit account to protect them when responding to a valid garnishment order.

The CFPB enforcement action against Bank of America resulted from what the CFPB deemed to be Bank of America's processing of illegal out of state garnishment orders. Over the course of more than 10 years, the CFPB found that Bank of America's processes for handling out of state garnishments were unfair or deceptive in a number of ways:

- Not Honoring the Location of Consumer Accounts: Bank of America's account disclosures provided that the consumer's account would be located at the branch where the account was opened. However, the CFPB found that the bank had a practice of treating any garnishment notice it received, as long as it was issued in a state where Bank of America maintained a branch location, as applying to any consumer account, regardless of whether that account was located in that same state.
- Failing to Apply Applicable Exemptions: As mentioned above, many states exempt funds from garnishment. Bank of America often applied the exemption law of the state that issued the garnishment, instead of the exemption law of the place where the account was located or where the customer resided.
- Misleading and Unenforceable Account Disclosures: Bank of America included language in its account disclosures that "directed" Bank of America not to contest any legal process it received and waived any liability for Bank of America's acceptance of and compliance with any legal process. Bank of America used these provisions to reject complaints from customers whose accounts were depleted in response to out-of-state garnishments, even where Bank of America's compliance was in violation of the law of customer's state of residence.

In response to Bank of America's conduct, the CFPB ordered the bank to:

- Refund at least $592,000 in garnishment fees that were charged to customers where garnishments were Bank of America's compliance was unlawful.
- Review and reform its garnishment compliance system, including notifying courts when an account is located out of state.
- Eliminate language from its account disclosures that attempt to limit a customer's right to challenge garnishments.
- Pay a $10 million fine to the CFPB.

This Bank of America case provides a cautionary tale to financial institutions everywhere, but particularly those financial institutions that serve or are located in California, as California maintains strong legal protections for its consumers. In addition to the various exemptions that apply to bank account levies, California is also a state that does not typically honor out of state court judgments without some sort of authentication or hearing that occurs in a California state court.

As you review your financial institution's processes and procedures for handling garnishments, please keep in mind the following:

- The CFPB identified at least 4 states that currently are "Restriction States" that prohibit garnishment of out of state accounts: Alabama, California, Florida, and Oregon. Particular caution should be exercised when dealing with levies or garnishments from or pertaining to residents of these states.
- Employee training in this area is key. While Bank of America maintained procedures that appeared to appropriately identify states where out of state garnishments were problematic, employees were still processing these garnishments in violation of Bank of America policy and applicable law.
- This is not an area where financial institutions can contract around their obligation to comply with state legal requirements regarding exemptions and state court jurisdiction. Financial institutions should review their disclosures to ensure such provisions do not appear, and to the extent disclosures do have some language that attempts to have customers waive their legal protections, such provisions should not be enforced.

Because state law is subject to change, financial institutions should ensure that they regularly review their out of state garnishment procedures, and, if necessary, reach out to counsel to obtain updated compliance advice.