ATTORNEYS AT LAW
SW&M

LEGAL ISSUES BULLETIN

October 2021

ATTORNEY-CLIENT PRIVILEGE – NOT TO BE CIRCULATED
FOR ADDRESSEE USE ONLY

T.D. Bank EFTA Class Action Claim

In *Jimenez v. T.D. Bank, N.A.*, a putative class action was brought by a group of individuals who held accounts with T.D. Bank, alleging that T.D. Bank closed, then reopened bank accounts in Plaintiffs' names without authorization. In particular, the plaintiffs asserted claims for breach of contract and the implied covenant of good faith and fair dealing, unjust enrichment, conversion, and violations of the FCRA, the EFTA, and Massachusetts Consumer Protection law. T.D. Bank filed a motion to dismiss the plaintiffs' complaint, which was ultimately granted in part and denied in part.

Importantly, T.D. Bank's motion to dismiss was denied as to claims that it opened accounts in plaintiffs' names without their permission and seized funds and fees. The *Jimenez* court held that such conduct might be unlawful under the EFTA. Specifically, the court held that the plaintiffs' complaint may proceed regarding the allegations that T.D. Bank violated § 1693i(a) of the EFTA: "[n]o person may issue to a consumer any card, code, or other means of access to such consumer's account for the purpose of initiating an electronic fund transfer other than (1) in response to a request or application therefor; or (2) as a renewal of, or in substitution for, an accepted card, code, or other means of access, whether issued by the initial issuer or a successor." In sum, the court held that T.D. Bank may have violated the EFTA by issuing unauthorized means of access to customer accounts by reopening closed accounts without the plaintiffs' authorization to initiate electronic fund transfers. Based on the foregoing, we recommend that financial institutions review their policies and procedures regarding the closure and reopening of accounts and ensure that such policies comply with applicable laws, including the EFTA.

Recent Court Decisions Further Restrict TCPA

This year several federal court cases have clarified the definition of an automatic telephone dialing system (ATDS) under the Telephone Consumer Protection Act (TCPA). These cases provide valuable guidelines for businesses seeking to make routine computer-aided calls to their customers without risking costly TCPA litigation.

Earlier this year, in *Facebook, Inc. v. Duguid*, the United States Supreme Court resolved a split in authority and held that TCPA's plain meaning was that it only applied to equipment that uses a "random or sequential number generator" to dial phone numbers.. The case arose from Facebook sending notification messages to phone numbers when someone logged in from an unknown device. Duguid did not have a Facebook account and never gave Facebook his phone number but was repeatedly contacted about an individual trying to access his Facebook account from an unknown device. He ultimately sued for a TCPA violation.

The Supreme Court dialed back the 9th Circuit and others as to the definition of ATDS as equipment with the capacity both "to store or produce telephone numbers to be called using a random or sequential number generator" and to dial those numbers, ruling that various Circuits had impermissibly expanded the definition by finding that it included any system which could automatically dial saved numbers. Subsequently, several District court cases have further refined and clarified the definition of an ATDS based on the strict statutory interpretation in *Duguid*. These include rulings that:

- Software operating based on identification codes, rather than phone numbers, did not trigger TCPA protection;
- Birthday messages could not be randomly, as the numbers were on specific occasions and generated from a specific list; and
- Various factors may now indicate whether an automated call or text falls within the TCPA protections. These factors include, among others, whether the communication was impersonal and generic or there were multiple repetitive messages in a short period.

Collectively, these cases erode the prior broad interpretation of the TCPA and provide a much clearer framework for businesses to follow when deciding to place automated calls.

USAA Mobile Deposit Patent Infringement Update

After winning $200 million against Wells Fargo and filing suit against PNC Bank for patent infringement, it appears USAA's efforts will not stop there. It seems that USAA has recently begun to directly reach out to a number of financial institutions via cold calls. We understand USAA is attempting to engage in conversations with financial institutions using remote deposit capture (RDC) technology to enter into licensing arrangements for its patent portfolio, which, in turn, would provide protection from being sued by USAA for infringement. However, prior to any discussions, USAA is requiring that financial institutions sign an NDA. If signed, the financial institution would be prohibited from discussing the terms of the licensing arrangement made with USAA, including pricing, with any third parties, including its service providers. So, the financial institution would be unable to attempt to seek any recourse from its vendor from which it purchases the RDC technology and could jeopardize the infringement indemnity protections under existing contracts. It seems USAA is attempting to capitalize on the fear of being sued in an effort to persuade financial institutions to pay USAA for such protection, regardless of the

fact that the financial institution may be able to seek indemnification from its vendor. Accordingly, we strongly encourage financial institutions to consult with legal counsel prior to entering into an NDA and engaging in such discussions with USAA.

OFAC Issues Updated Advisory

On September 21, the Office of Foreign Asset Control (OFAC) issued an updated advisory regarding the sanctions risks associated with ransomware payments in connection with malicious cyber-enabled activities. The updated advisory did not materially alter OFAC's October 2020 guidance on the same topic but instead reiterated the strong stance that companies should not make ransomware payments. The advisory did provide a more robust discussion of mitigating factors and identified an additional mitigating factor not outlined in October 2020. Per the September 2021 advisory, the two mitigating factors that OFAC will consider in any enforcement action involving a cyber ransom payment are (1) defensive/resilience measures taken by the company, and (2) cooperation with OFAC/law enforcement.

With respect to the defensive/resilience measures mitigating factor, OFAC encourages financial institutions and other companies to "implement a risk-based compliance program to mitigate exposure to sanctions-related violations," which, in particular, accounts for the risk that a ransomware payment may involve a person on OFAC's SDN List, another blocked person, or a comprehensively embargoed jurisdiction. "Meaningful steps taken to reduce the risk of extortion by a sanctioned actor through adopting or improving cybersecurity practices, such as those highlighted in the Cybersecurity and Infrastructure Security Agency's (CISA) September 2020 Ransomware Guide, will be considered a significant mitigating factor in any OFAC enforcement response." These "meaningful steps" may include, among other things, "maintaining offline backups of data, developing incident response plans, instituting cybersecurity training, regularly updating antivirus and anti-malware software, and employing authentication protocols."

The other new mitigating factor is that OFAC will consider the reporting of ransomware attacks to appropriate U.S. government agencies, the nature and extent of a company's cooperation with OFAC, law enforcement, and other relevant agencies, and whether an apparent violation of U.S. sanctions is voluntarily disclosed. Where payments may have a sanctions nexus, a company's self-initiated and complete reporting of a ransomware attack to relevant government agencies, made as soon as possible after the attack is discovered, will be considered a significant mitigating factor in determining an appropriate enforcement response. A company's full and continuing cooperation with law enforcement by, among other things, providing all relevant information (including technical details, etc.) will also be considered.

Where the mitigating steps described above have been taken, OFAC is more likely to resolve apparent violations with a non-public response (i.e., a No Action Letter or a Cautionary Letter).

Mandatory Employment Arbitration Agreements

On September 15, the 9th Circuit vacated an injunction prohibiting the enforcement of AB-51, which related to mandatory arbitration agreements. Specifically, AB-51 prohibits an employer from requiring employees or applicants to sign mandatory arbitration agreements waiving any right, forum, or procedure for a violation of any provision of the California Fair Employment and Housing Act (FEHA) or other specific statutes governing employment (e.g., the California Labor Code). Previously, a district court held that AB-51 is preempted by the Federal Arbitration Act (FAA) and imposed a preliminary injunction barring the law from going into effect. However, the 9th Circuit reversed the lower court's decision and held that the FAA preempts AB-51 only to the extent AB-51 seeks to impose civil or criminal penalties on employers who have executed arbitration agreements covered by the FAA.

Not surprisingly, the U.S. Chamber of Commerce has filed a petition for a rehearing. During this time, the injunction will remain in effect. We will continue to monitor this case for any developments. Any financial institutions desiring the use of mandatory arbitration agreements should consult legal counsel.

ADU Lending

Continuing steady expansion of Accessory Dwelling Unit popularity and flexibility in California, 2020 and 2021 brought numerous new laws in this area. The boom has brought the next big trend—ADU lending—with FinTech companies jumping to get lenders and borrowers onboard. Strong compliance and product design measures are important in this area, with underwriting, appraisal, recording, and draw management elements requiring construction-loan-esque preparation and attention. Financial institutions looking into these products should carefully review contracts and procedures to promote safe and sound adoption of this latest product development.

California Credit Union Charter Modernization (SB269)

A long awaited modernization bill passed, bringing a measure of regulatory relief to California chartered credit unions. Two important elements of the bill will be effective January 1, 2022: (a) allowances for expulsion of members without requiring member meetings; and (b) revising Financial Code 15050 to bring back permissibility of employee loan discounts for CEOs and Credit Managers. As to the first, many credit unions will need to amend their Bylaws and policies to take advantage of the new law. As to the second, credit unions that curtailed loan discounts for executives since 2017 should refresh discount certificates and any tax analysis necessary if loan discounts are a part of their compensation packages.