Legislative Update 248

November 1, 2024

Highlights this issue:

- On October 22, the Consumer Financial Protection Bureau (CFPB) finalized its personal data rights rule requiring data providers to allow consumers the ability to port financial information. The initiative comes from a requirement under the Dodd-Frank Act for the CFPB to implement rules for financial data sharing and largely adheres to proposed rules from last October.
- On October 16, the Federal Trade Commission (FTC) finalized its "click-to-cancel" rule ("final rule") to make it easier for consumers to cancel their enrollment in subscriptions. FTC Chair Lina Khan stated that businesses often make it challenging for consumers to cancel their subscriptions and that the final rule will stop "tricks and traps," save Americans time and money, and help ensure the consumers do not have to pay for services they no longer want.
- On October 21, the Department of Justice (DOJ) published a Notice of Proposed Rulemaking (NPRM) to implement President Joe Biden's Executive Order on "Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern."
- On October 10, the New Jersey Attorney General's Division of Consumer Affairs announced a proposed rule implementing disclosure requirements for national consumer reporting agencies. Under the 2019 law, a consumer reporting agency that compiles and maintains files on a nationwide basis must make the disclosures available to a consumer in Spanish and any other language determined through rulemaking.

FEDERAL UPDATE

CFPB finalizes personal financial data rights rule

On October 22, the Consumer Financial Protection Bureau (CFPB) finalized its personal data rights rule requiring data providers to allow consumers the ability to port financial information. The initiative comes from a requirement under the Dodd-Frank Act for the CFPB to implement rules for financial data sharing and largely adheres to proposed rules from last October. The rule will apply to Regulation E covered deposit accounts and Regulation Z covered credit card accounts and require the building of developer interfaces to help ensure consumers can access or authorize a third-party to obtain personal financial data. Additionally, the rule further prohibits data providers from

assessing any fees to consumers or third parties for accessing covered data; mandates that authorized third parties adhere to certain consumer disclosure, consent, data retention, and data security requirements; broadly prohibits the use of consumer data for any secondary purposes and permits data providers to restrict screen scraping access once they establish a developer interface.

In a speech announcing the final rule, CFPB Director Rohit Chopra stated that the CFPB expects to advance additional rules to apply to more products, services, and use cases; encouraging competition by allowing consumers to more easily switch banks or providers and choose the best deal. The final rule includes a tiered compliance schedule, giving larger firms until April 1, 2026, to comply, while smaller entities will have until April 1, 2030. Depository institutions with assets of $850 million or less are exempt from the rule's requirements. Less than 24 hours after the publishing of the rule, the Bank Policy Institute filed a lawsuit to stop the rule.

FTC issues final rule on "click-to-cancel"

On October 16, the Federal Trade Commission (FTC) finalized its "click-to-cancel" rule ("final rule") to make it easier for consumers to cancel their enrollment in subscriptions. FTC Chair Lina Khan stated that businesses often make it challenging for consumers to cancel their subscriptions and that the final rule will stop "tricks and traps," save Americans time and money, and help ensure the consumers do not have to pay for services they no longer want. The final rule provides a consumer protection framework to prohibit sellers from:

- misrepresenting any material fact made while marketing goods or services with a negative option feature:
- failing to clearly and conspicuously disclose material terms prior to obtaining a consumer's billing information in connection with a negative option feature:
- failing to obtain a consumer's express informed consent to the negative option feature before charging the consumer; and
- failing to provide a simple mechanism to cancel the negative option feature and immediately halt charges.

The announcement noted that the Commission received thousands of complaints about negative options and recurring subscription practices. The Commission voted 3-2 to adopt the final rule, with Commissioners Melissa Holyoak and Andrew Ferguson voting no. The final rule will go into effect 180 days after it is published in the Federal Register. On October 24, NCTA – the cable and internet provider trade association - filed a lawsuit to block the rule. The lawsuit describes the move as "arbitrary, capricious, and an abuse of discretion," arguing that a multistep cancellation process protects customers and allows companies to offer them better deals. The lawsuit is also supported by the Electronic Security Association and the Interactive Advertising Bureau.

DOJ publishes NPRM on national security risks posed to U.S. bulk sensitive personal data

On October 21, the Department of Justice (DOJ) published a Notice of Proposed Rulemaking (NPRM) to implement President Joe Biden's Executive Order on "Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern." The NPRM would implement the Executive Order by creating categorial rules for data transactions that pose a risk of providing countries of concern access to bulk U.S. sensitive personal data or government-related data. The rule would also identify restricted transactions and classes of exempt transactions, specify countries of concern and classes of covered persons to whom the proposed rule applies, create processes to issue licenses authorizing certain restricted transactions. The proposed rule would require employment, investment, and vendor agreements that qualify as restricted transactions to comply with CISA's proposed security requirements, which would require U.S. citizens engaging in restricted transaction to comply with organizational cybersecurity policies and data minimization methods. The DOJ's National Security Division is requesting public comments from industry, trade associate groups, and other entities within 30 days of its publication in the Federal Register.

CFPB publishes guidance to protect consumers from unchecked worker "surveillance" methods

On October 24, the CFPB issued guidance to safeguard workers from "unchecked" digital tracking and "opaque" decision-making systems. The guidance addresses whether an employer can make employment decisions utilizing background dossiers, algorithmic score, and other third-party reports about workers without adhering to the Fair Credit Reporting Act. The guidance states that, similar to credit reports and scores, information used by employers to make hiring decisions, promotion, reassignment, or retention decisions can be regulated by the FCRA. The CFPB states that whether an employer that makes employment decision based on a report from a third party is regulated by the FCRA, enforcers should consider 1) does the employers use of data qualify as a use for employment purposes under the FCRA; and 2) is the report obtained by a consumer reporting agency. In its statement announcing the guidance, the CFPB notes that consumer reports may be used to predict worker behavior, reassign workers based on performance, issue warnings or other disciplinary actions, and evaluate social media activity. The CFPB called on employers to review their current use of third-party consumer reports to help ensure compliance with the FCRA.

President Biden issues national security memorandum on AI to enhance national security

On October 24, President Joe Biden issued a National Security Memorandum (NSM) on Artificial Intelligence. The White House also released a fact sheet on the NSM stating that AI will have significant implications for national security and foreign policy in the near future and seeks to build on the previous Executive Order to drive the safe, secure, and trustworthy development of AI. The NSM orders the U.S. government to help ensure

that the United States leads internationally in the development of AI and use technologies to further the government's national security mission. The NSM aims to shape international standards regarding AI usage to reflect democratic values such as privacy, human and civil rights, and civil liberties. The NSM focuses on securing chip supply and other vital supply chain bottlenecks, developing research organizations, and facilitation inter-agency collaboration.

STATE UPDATES

New Jersey issues proposed rule on CRA multiple language disclosures
On October 10, the New Jersey Attorney General's Division of Consumer Affairs announced a proposed rule implementing disclosure requirements for national consumer reporting agencies. Under the 2019 law, a consumer reporting agency that compiles and maintains files on a nationwide basis must make the disclosures available to a consumer in Spanish and any other language determined through rulemaking. While the law required at least ten languages other than English and Spanish - the proposed rule provides that reports should be provided in English, Spanish, and any six languages that are determined by the Division of Consumer Affairs to be a first language of a significant number of consumers. The proposed rule cites recent litigation as a reason to pare back the number of available languages. The list of languages must be updated annually by the Division and consumer reporting agencies must make the updated disclosures available by June 30 of the following year. Experian is reviewing the proposed rule with public comments due in early December.

Michigan Senate advances judicial privacy
On October 23, the Michigan Senate Judicial Committee advanced an amended HB 5724 regarding judicial privacy. The legislation follows recent frameworks in Minnesota and Wisconsin allowing a judge to request that a public body or person not publicly post or display the personal identifying information of a judge or a judge's immediate family member. A judge may submit a written request, on a form prescribed by the state court administrative office, to a public body or person to remove a public posting or display of personal identifying information of the judge or the judge's immediate family member. Once a person receives the request, the personal information may not be publicly posted, displayed, or transfer the personal information. If the personal information is publicly posted, the information must be removed within five business days. If a person is not in compliance with this measure, the judge or the judge's immediate family member may commence a civil action for injunctive relief. The legislation provides exceptions for information subject to the FCRA, GLBA, and HIPPA. Further, data used for fraud purposes is exempt if the information is not disseminated to the public or publicly posted. The bill is eligible for further consideration by the full Senate. Experian continues to work with CDIA to seek alignment of state data privacy laws.

New York Department of Financial Services releases guidance on AI-related cybersecurity risks
On October 16, the New York State Department of Financial Services (DFS) released new guidance to help regulated entities address and mitigate cybersecurity risks associated with artificial intelligence (AI). The guidance seeks to address inquiries received by the Department regarding AI's impact on existing cybersecurity regulations. Under the guidance, DFS identifies two categories of cybersecurity risk specific to AI: 1) risk caused by threat actors' use of AI; and 2) risk caused by a covered entity's use or reliance upon AI. Using the cybersecurity framework, DFS outlines several measures to combat AI related risk, including applying robust controls to combat social engineering,

implementing third party vendor and supplier policies, and enforcing data minimization requirements in case multifactor authentication fails. The guidance notes it does not impose new requirements but is intended to help DFS-regulated institutions meet existing compliance obligations.