New York State
Department of Financial Services

Report on Investigation of Facebook Inc. Data Privacy Concerns

February 18, 2021

The advent of the digital age has exponentially expanded the scope and scale of information that businesses collect on consumers. Prior to the digital revolution, the information that a business could, as a practical matter, collect about consumers was limited and, generally speaking, relatively obvious to the consumer. The most common data collected — data concerning transactions, information gleaned from loyalty rewards programs and the like, and information pertinent to credit decisions — directly related to interactions between the consumer and the business and generally did not give rise to significant privacy concerns. That has changed dramatically in an age when consumers are using the Internet, mobile applications, and social media platforms to facilitate interactions throughout their daily lives. The purchases we make, the news we read, the issues we engage with, and even the way we connect with friends and family all leave digital footprints, and technology companies are often tracking, analyzing, and using that information in ways that are not at all apparent to consumers. This investigation sheds light on this important issue.

On February 22, 2019, The Wall Street Journal published an article reporting that Facebook, Inc. ("Facebook") was receiving sensitive, personal user data from at least 11 popular mobile application, or "apps" (the "WSJ Article").[1] According to the WSJ Article, data being sent to Facebook included information such as users' heart rates, blood pressure readings, menstrual cycles, and even pregnancy statuses. In one such case, Flo Health, Inc. ("Flo"), a menstruation and fertility-tracking app used by more than 100 million consumers, sent Facebook data every time a user logged a period or told the app that she intended to get pregnant. The app would also send data whenever it was opened, apprising Facebook of where the user was in her menstrual cycle — noting "ordinary" or "period" to "ovulation" or "pregnant."

[1] S. Schechner & M. Secada, You Give Apps Sensitive Personal Information. Then They Tell Facebook., WSJ (Feb. 22, 2019).

Following the WSJ Article's publication, New York Governor Andrew M. Cuomo called on the New York State Department of Financial Services ("DFS" or the "Department"), which licenses Facebook Payments, Inc. ("Facebook Payments"), a wholly owned Facebook subsidiary, to investigate these allegations, calling the conduct an "outrageous abuse of privacy."[2] He also called on the relevant federal regulators to become involved. In a statement, Facebook expressed its intent to assist the State's probe, but took no responsibility for the conduct alleged by the WSJ, noting that the WSJ Article reported on how other apps use people's data to create ads, not Facebook.

This Report summarizes the Department's investigation into the privacy concerns raised by the WSJ Article, the remediation measures Facebook has taken as a result of the Department's investigation, and the Department's recommendations for further action.

Part I of this Report summarizes the roles of the Facebook entities involved and discusses how Facebook obtains data from third-party app developers.

Part II provides a brief overview of the Department's investigation and discusses the extent to which Facebook cooperated with the Department's inquiries. As discussed below, Facebook did indeed receive sensitive user data from third-parties, in contravention of Facebook's own internal policies, particularly in the area of medical and health information. Though Facebook generally cooperated with the Department's investigation, it refused to undertake an appropriate "look-back" review that would have provided details about the scope and scale of the improper transfer of sensitive personal information.

Part III outlines the remedial measures that Facebook has undertaken as a result of the Department's investigation to address the privacy issues implicated here, including (1) enhancing

[2] Reuters Staff, NY Governor Orders Probe into Facebook Access to Data from Other Apps, REUTERS (Feb. 22, 2019).

Facebook's detection and blocking of sensitive data received from developers using Facebook's new Health Terms Integrity System; and (2) providing additional educational resources for developers to better inform them of their obligations not to transmit sensitive information. This section also describes Facebook's recently launched "Off-Facebook Activity" feature, which provides users with greater control over their online data.

Part IV provides the Department's recommendations for ongoing and additional remediation of the concerns described in this Report, including increased focus on app developer controls, more effective enforcement of Facebook's policies and procedures, and the need for enhanced regulatory oversight for social media giants and other data analytics companies.

I. Background

A. Facebook Generally

Facebook is a social media corporation based in Menlo Park, California. It is one of the world's most valuable companies and is considered to be one of the "Big Five" technology companies, along with Microsoft, Amazon, Apple, and Google. Facebook ranked No. 46 in the 2020 Fortune 500 list of the largest United States corporations by revenue, the vast majority of which comes from advertising. In 2019, Facebook's ad revenues were approximately $69.66 billion USD, accounting for about 98.5 percent of its global revenue. Facebook offers numerous products and services beyond its social networking platform, including Facebook Messenger, Facebook Watch, Facebook Portal, Facebook Business Tools, and Facebook Payments.

Facebook Payments, a wholly owned subsidiary of Facebook, allows users of Facebook products to send money to and receive money from other Facebook users, make certain charitable donations, and make purchases or in-app upgrades while playing games online using

Facebook. Facebook claims that it is able to offer these services to its users free of charge in significant part because of the ad revenue it collects through other Facebook products. Facebook Payments has been licensed by the Department as a money transmitter since 2013.

B. Facebook's Business Tools and Software

Online analytics services allow website owners, app developers, and advertisers to provide targeted advertising to users by learning more about consumers' usage of their apps, such as how many users opened their app on a particular day or how many purchases were made in the app in a particular period. Website owners and app developers program their software to collect certain data about users, which is then sent to the analytics service. The analytics service then provides the developer with analysis of that usage data, often linked with other data that the analytics service has on a given user. Some companies offer these analytics services for a fee; others, as in the case of Facebook, provide the analytics services free of charge as a way to drive ad revenue on their own related platforms.

Facebook offers app developers who download Facebook's Software Development Kit ("SDK") access to free online data analytics services. One of the Business Tools available in the SDK is called "App Events." App Events allows app developers to integrate Facebook with their app by automatically transmitting data from the mobile app or website to Facebook so that the data can be analyzed. An app coded through Facebook's SDK will automatically transmit a set of basic information to Facebook, including user device information — such as a device's IP address and type, the time of use, and a device's advertising ID — which companies can then use to build a marketing profile for each user. In addition, using the App Events tool, apps will also automatically send Facebook information about certain basic actions called "events" that users

take on their app as well, such as opening the app, clicking, swiping, viewing certain pages, placing items into a checkout, and so on.

In addition to such standard information, app developers can also produce custom analytics metrics by creating a custom category of information, called a "Custom Event." Often, the Custom Event is linked to a field in the app or website that calls for user-supplied information, such as a search, a fillable data field, or a pulldown menu. The Custom Event data Facebook receives from each app is then stored on Facebook servers for analysis. The resulting analysis helps app developers understand how people use their services, which can then be used for their own advertising and marketing purposes, generating additional revenue both on and off Facebook. The sensitive user data being shared with Facebook, as reported in the WSJ Article, consisted of "Custom Event" data that was accessed and transmitted through the App Events tool.

C. Facebook's Data Policy and Business Tool Terms

Facebook's Data Policy, which describes the information Facebook processes to support Facebook, Instagram, Messenger, and other products and features offered by Facebook, outlines the many ways in which Facebook collects information about Facebook users — in addition to information a user may voluntarily share with Facebook while using its social media platform. For example, Facebook collects information from its users through metadata embedded in the content a user provides, what a user sees through features such as Facebook or Instagram's Camera, and information shared with other users through personal messages. Facebook also collects information about a user's activity off Facebook, such as which websites a user visits and the ads a user sees, as well as a variety of information about the computers, phones, and other web-connected devices consumers use to integrate with Facebook Products. Facebook then

combines the data it collects across different devices to personalize the content a user sees on the Facebook platform, facilitate targeted advertising for each user, and analyze any actions the user may have taken in response to targeted ads or personalized content. It uses the information it collects to provide analytics, such as aggregated statistics and insights, for its advertisers and other third-party partners.

Facebook's Business Tools Terms outlines the types of information it collects from third-party partners. Using Facebook's Business Tools, advertisers, app developers, and publishers share information with Facebook about a user's activities off Facebook, regardless of whether a user is logged into Facebook or even has a Facebook account. Facebook's Business Tools Terms places responsibility on its partners to ensure that they have the legal right to collect, use, and share user data before providing it to Facebook, and the agreement permitting usage of the Facebook SDK further requires developers to ensure that they have the right to share any information that they transmit. Facebook asserts that it does not sell any user information to anyone and imposes strict restrictions on how its partners can use and disclose the data it provides. Significantly, Facebook's Business Tools Terms also prohibit app developers and other third parties from sending Facebook sensitive data, such as health related data, information concerning a user's religious practices or other personal information:

> You will not share Customer Data with us that you know or reasonably should know is from or about children under the age of 13 or that includes health, financial information, or other categories of sensitive information (including any information defined as sensitive under applicable law).

II. The Department's Investigation and Facebook's Cooperation With That Investigation

Following the publication of the WSJ Article and Governor Cuomo's call to action, the Department commenced an investigation to evaluate the significance of the conduct described by the WSJ in relation to its licensee, Facebook Payments. The Department sent a letter to Facebook and Facebook Payments requesting documents and information in connection with its investigation into the privacy concerns related to Facebook's SDK. In addition, the Department sent similar letters to each of the apps that were identified in the WSJ Article, requesting the production of documents and information.

It quickly became clear that DFS's licensee, Facebook Payments, had no involvement in the privacy issues being examined — Facebook Payments plays no direct role in the collection, transmission, or analysis of the kinds of data at issue. All of the problematic data is collected and analyzed by the parent company, Facebook. Facebook has repeatedly indicated its willingness to cooperate fully with the Department so that DFS could conduct its investigation. Facebook's record on living up to that commitment, unfortunately, has been mixed.

On the positive side, Facebook provided the Department with information, both in the form of documents and presentations from subject-matter experts, on how Facebook, through its SDK, receives data from app developers, as detailed in the prior section. In that process, Facebook acknowledged to DFS that, until DFS commenced its investigation, Facebook routinely obtained sensitive data from app developers, particularly in the area of health-related information, contrary to its own policies. Essentially, notwithstanding Facebook's policy that app developers should not transmit sensitive data to Facebook, there were many examples where the developers violated that policy and Facebook did indeed — unwittingly, it contends — receive, store, and analyze sensitive data. The information provided by Facebook has made it clear that

Facebook's internal controls on this issue have been very limited and were not effective at enforcing Facebook's policy or preventing the receipt of sensitive data.

In addition to acknowledging the problem, Facebook has engaged with the Department to discuss changes in their procedures that would address the issue. As discussed more fully in the next section, as a result of DFS's investigation, Facebook has (a) built and implemented a screening system that is designed to identify and block sensitive information before it enters the Facebook system; and (b) enhanced app developer education to better inform developers of their obligations to avoid transmitting sensitive data. Facebook has also taken steps to better inform its users about, and give them more control over, data that is collected about them, including from off-Facebook activity.

On the other hand, notwithstanding Facebook's assertions that it wanted to cooperate fully with the Department's investigation, Facebook has repeatedly rebuffed DFS's efforts to obtain information that would have provided more fulsome transparency with respect to the scope and scale of the problem. Though Facebook acknowledges the problem — *i.e.*, that in the past it did receive sensitive information from app developers contrary to its own policy — it has failed to provide sufficient detail about, among other things, specifically what kinds of sensitive information was obtained, how regularly it was received, or which app developers violated the rules by transmitting such information.

To shed light on these issues, the Department asked Facebook to undertake a comprehensive "look-back" review to query the data that it had received during a particular period in the past so that these details could be examined, both for the purpose of providing transparency to the public and to ensure that the remediation efforts were actually addressing the full scope of the problem. Facebook objected, however, on the basis that such a look-back review

was too "burdensome" and that it did not have an existing functionality to go back and review data it received. Though the Department found it curious, to say the least, that one of the leading data analysis companies in the world would find it difficult to analyze its own data, the Department nonetheless engaged with Facebook to arrive at a reasonable look-back plan that would provide the transparency that DFS was looking for while minimizing the burden on Facebook. Contrary to its commitment to fully cooperate, however, Facebook ultimately chose not to engage in a fulsome look-back review. It is unclear whether Facebook was unwilling to expend the time and resources to undertake this review or simply did not want a regulator to gain access to such information, but whatever the motivation, the result is that Facebook has failed to engage fully with respect to this issue. DFS calls on federal regulators with nationwide jurisdiction over Facebook to compel Facebook to provide full transparency on this issue.

III. Facebook's Remediation Efforts Resulting From the Department's Investigation

In response to the DFS investigation, Facebook proposed to the Department several avenues for remediation of the Department's concerns regarding third-party sharing of sensitive user information. Following those discussions, Facebook undertook several significant remediation efforts to address the issues identified by the Department's investigation, including: (1) enhanced detection of sensitive health data through Facebook's New Health Terms Integrity System; and (2) enhanced app developer education. Additionally, the introduction of Off-Facebook Activity, which was under development when the DFS investigation started, has further addressed some of the Department's concerns.

A. Facebook's Health Terms Integrity System

In the summer of 2019, following its initial discussions with the Department, Facebook began developing a program that would identify and block certain sensitive user information

being sent to Facebook, such as health-related terms used in apps Custom Event fields (the "Integrity System").[3] The Integrity System utilizes two complementary components, exact-match blocking and machine-learning to identify and block sensitive data.

During the exact-match blocking phase, the Integrity System first identifies apps that are likely to send sensitive data using a combination of factors, such as the name of the app, the language describing the app on the app store, and the app's classification. The Integrity System, which runs daily, then analyzes data that is transmitted by those apps and compares it to a list of terms that Facebook deems likely to be sensitive (the "Block List"). If data from one of the reviewed apps matches a term on the Block List, the program blocks such data from storage and use by Facebook's systems. The Block List, which now includes more than 70,000 terms from health and medical texts and sources, covers areas including:

- Diseases, medical conditions, and injuries;
- Sexual and reproductive health;
- Mental health and psychological states;
- Types of medical devices and health trackers;
- Medical procedures / treatments / testing;
- Medications / supplements (over the counter and prescription);
- Body specifications, bodily activities and biological cycles; and
- Physical locations that identify a health condition, or places of treatment / counseling.

For the second, machine-learning phase, Facebook has built a machine-learning system to identify and block potentially sensitive data that is not dependent on an exact match with Block

[3] Even before the Department's inquiry, Facebook had been blocking certain identification and financial-related data, such as credit card numbers, sent by apps through its Business Tools.

List terms. This component of the Integrity System analyzes terms on the Block List and is designed to learn to recognize, over time, terms that are likely to be similarly sensitive. For example, the machine-learning system analyzes the prescription drug names that appear on the Block List and will add new drug names and block them from being used in Facebook's systems, without a human engineer having to add the new names to the Block List. To do so, Facebook's engineers analyze the machine-learning model's results and provide feedback to the Integrity System regarding the accuracy of its predictions, both to avoid future false positive results and to ensure that the Integrity System is picking up all relevant sensitive data. Facebook began implementing its early machine-learning model in July 2020. Currently, the model runs in tandem with the exact match system so that Facebook can continue working on improving it while also using the Block List.

As of the conclusion of the Department's investigation, Facebook indicated that the Integrity System is not yet operating with complete accuracy and explained that filtering sensitive terms requires additional testing due to the volume and complexity of information being processed. For example, because the system identifies terms for the potential that they are used by an app in connection with a health status, the system can be overinclusive in that it detects and removes terms regardless of whether the words are actually sensitive: a health charity may track its fundraisers, creating the Custom Event "Cancer Society," which would then be flagged and removed by the Integrity System — even though the word "cancer," as used in this context, would not relate to a user's health status. The system could also miss certain terms in the sense that a term may not be on the Block List or the machine model may not learn it is sensitive. More fundamentally, the current version of the Integrity System is built to screen and block sensitive data in a single category — health-related data. The current search terms are also

presented in English only, but Facebook has indicated a plan to add terms in other languages at a later time.

The number of Custom Events that trigger the Integrity System daily is staggering: Facebook reported to the Department that from November 21-28, 2020, for example, a daily average of approximately 25 million events sent by health apps triggered the system, which represents only approximately 2.5% of the daily total number of events sent by health apps during that same time. Facebook's stated goal is to expand the Integrity System and add more categories across all apps once fully operational, with the next area of focus being the identification of financial information. Facebook has indicated that it is still considering what other common forms or combinations of data the Integrity System can learn to identify as financially related.

B. Enhanced App Developer Education

During the course of the Department's investigation, DFS asked Facebook to consider ways to provide app developers with enhanced guidance in order to make their obligations to prevent the transmission of sensitive data to Facebook clearer and more tangible. To that end, Facebook has recently published Business Help Center guides containing information that describes in greater detail what data — including data pertaining to health — Facebook considers potentially sensitive and thus should not be sent to Facebook according to its Business Tools Terms. Materials available through Facebook's Business Help Center have been updated to include information outlining what constitutes restricted Facebook Business Tools data; sensitive health information; personally identifiable information (PII); and a quick-reference guide for developers on what their next steps should be if their data has been flagged as violating Facebook's policies.

Additional measures to better inform developers as to their data privacy obligations were still under discussion as of the conclusion of the DFS investigation, and Facebook indicated that one proposal it was considering included educating the internal Facebook teams that work closely with app developers on their technical questions regarding Facebook's privacy and data sharing policies. Facebook also indicated that it was considering making the developer obligations more prominent in the Business Tools interface by adding reminders, additional links to educational materials, or banner notifications in well-trafficked areas.

C. Off-Facebook Activity

Beginning in January 2020 in the United States, Facebook launched the "Off-Facebook Activity" tool. That tool gives Facebook users more visibility into the information that Facebook receives, among other things, from the apps that are using Facebook's Business Tools.

First, through Off-Facebook Activity users can view information that apps have sent Facebook about their activity off the Facebook platform. Specifically, through the "Manage Your Off-Facebook Activity" page in the Facebook app, users can view a list of apps that have shared their activities with Facebook and a high-level summary of the information shared by these apps, including the number of App Events that Facebook received regarding the user from each app. Moreover, users can navigate from this page to the "Download Your Information" tool (which existed prior to Off-Facebook Activity's launch) to view even more specific information about the data Facebook receives from apps. The Download Your Information Tool allows users to download App Events data sent by apps to Facebook at the event-level, including the app that sent each event, the date and time Facebook received each event, and the name of each event.

Second, the Off-Facebook Activity tool provides users with the option to "Clear History," which allows users to disconnect their history of activity data, including sensitive App Events

data previously sent by health apps to Facebook, from being associated with their account. After users clear their history, this past data associated with their actions on an app can no longer generate targeted ads for that user on the Facebook platform.

Third, the Off-Facebook Activity tool allows users to select the "Manage Future Activity" option to change their association with apps going forward. In doing so, users can choose to "turn off" future connections between their Facebook account and their activities off the Facebook platform, for all apps or on an app-by-app basis. If users elect to turn off their future activity from an app, this prevents events data associated with a user's actions on that app from being used to generate targeted ads for that user on the Facebook platform.

IV. The Department's Recommendations

Although the remediation efforts described above are important first steps, the Department has identified several other steps that should be considered to prevent future disclosure of sensitive user data. These recommendations are not limited to Facebook, as it appears that the problematic data-sharing practices exposed in the WSJ Article are a continuing risk throughout the data analytics and social media industries. All companies within that industry — as well as the relevant regulatory bodies with oversight over those companies — should proactively take all reasonable steps to eliminate the practice of unauthorized sharing of sensitive user data with third-parties, whether they are business partners, advertisers or otherwise. The following paragraphs briefly summarize the Department's recommendations.

A. Stronger App Developer Controls

Although Facebook has taken some steps to improve developer education on this issue, as discussed above its primary remediation strategy has been to block sensitive data from reaching Facebook's systems on the back end of the system. Facebook could plainly do more on the front

end to prevent developers from transmitting sensitive data in the first place rather than relying so heavily on a back-end screening system that, no matter how sophisticated it is, will never be able to block all sensitive information.

As noted above, Facebook policy prohibits app developers from sharing with Facebook data that the developers "know or reasonably should know is from or about children under the age of 13 or that includes health, financial information, or other categories of sensitive information (including any information defined as sensitive under applicable law)." Although app developers must agree to these terms when they sign up for SDK, Facebook does little to ensure that developers are actually aware of this prohibition or to make particular note of it when the developers create the Custom Events that result in the transmission of sensitive data.

Facebook should be doing more to ensure that developers are fully aware of the prohibition not only when they sign up for SDK and agree to boilerplate conditions, but more meaningfully, specifically reminding developers at the time that they create Custom Events. Though there are no doubt many ways to make this policy more prominent, one suggestion is that Facebook program the SDK software so that every time an app developer attempts to create a Custom Event, a pop-up box requires the developer to certify in real time that the Custom Event field will not call for users to provide any of the categories of sensitive data. Such categories should include, at a minimum: PII; health information; financial information; religious affiliation; race and ethnicity; sexual preference; and information pertaining to children under 13.

Such a contemporaneous reminder, provided at the very moment that a developer is creating a Custom Event, has the potential of stopping improper transmissions of data before they are even set up, at least where the policy violation is caused by ignorance or a lack of attention on the part of the app developer. Significantly, this type of front-end control might

prevent the transmission of sensitive data that its back-end screening system simply would not catch.

Facebook has told the Department that implementing this suggestion would be technically challenging, but that it is considering whether there are additional places to remind developers of their obligations. DFS strongly urges Facebook to implement this suggestion or some other manner of providing a timely reminder of what data is prohibited.

B. Enforcement of Facebook's Policies

As noted, the sharing of sensitive user information by an app developer is a violation of Facebook Business Tools' terms of service. Merely stating a rule, however, has little meaning if the rule is not enforced, and the unfortunate fact is that Facebook does little to track whether app developers are violating this rule and takes no real action against developers that do. Although Facebook's Integrity System does make note of apps that have sent data that was dropped due to a hit from the Blocked List, Facebook's Integrity System, as it currently stands, makes no determination regarding whether a blocked term was sensitive and/or was transmitted in violation of Facebook's policies. Facebook has argued that, because it does not store data that is found to contain an exact match for a term on the Block List, it cannot determine whether a violation occurred or whether the term identified by the Integrity System merely was a false positive. Although an automated email is sent to the developer notifying them of the possible violation, no further effort is made to determine whether the dropped data was the result of a violation of Facebook policy, even for apps that repeatedly transmit data that is blocked.

The Department finds Facebook's efforts here seriously lacking and recommends that it undertake significant additional steps to police its own rules. Even assuming a strong screening program on the back end, Facebook must take steps to determine whether app developers are

transmitting sensitive data. An app developer that consistently tries to transmit sensitive data to Facebook but is repeatedly blocked by the Integrity System is still a significant risk to send problematic data that might get through the Integrity System screens. At the very least, for apps that have caused repeated blocks by the Integrity System, Facebook should implement some system to determine whether an actual violation has occurred, provide notice and an effective warning to those apps who have violated the policy, and impose an appropriate sanction, including removal from Facebook's systems, with respect to apps that continue to disregard the policy. Until there are real ramifications for violating Facebook's policies, Facebook will not be able to effectively prohibit the sharing of sensitive user data with third-parties.

C. Enhanced Regulatory Oversight

This troubling lack of privacy protection at Facebook illustrates a larger problem with the data analytics industry. The way Facebook receives and uses data from third parties is not unique to Facebook, and the issues identified in the WSJ Article are present to some extent throughout the data analytics industry. The problems uncovered in this Report clearly show that there is a need for more transparency and public oversight of the "big data" industry.

The Federal Trade Commission ("FTC") has recently taken some action on these issues. On December 14, 2020, the FTC announced that it would issue orders to nine social media and video streaming companies, including Facebook, requiring them to provide data on how they collect and use personal consumer information, their advertising and user engagement practices, and how their practices affect children and teens.[4] In addition, on January 13, 2021, the FTC entered into a Consent Agreement with Flo, the popular menstruation and fertility-tracking app reported on in the WSJ Article that used Facebook Business Tools. The FTC had alleged that Flo

[4] Federal Trade Commission Press Release, FTC Issues Orders to Nine Social Media and Video Streaming Services Seeking Data About How They Collect, Use, and Present Information (Dec. 14, 2020).

disclosed health data from millions of users to third parties that provided marketing and analytics services to the app, including Facebook's analytics division, after promising that such information would be kept private.[5]

Although the FTC's recent actions are steps in the right direction, it is painfully obvious that laws and regulations in this area have plainly not kept up with technological advancement, and even with respect to categories of data that any reasonable person would deem extremely private and out of bounds, consumers currently are not adequately protected. As recently noted in the Department's October 14, 2020, Twitter Investigation Report ("Twitter Report"),[6] the generally applicable laws that constitute the current legal framework for the regulation of social media giants and their data analytics divisions are blatantly insufficient. Though the Twitter report focused on data security and the lack of regulatory oversight for cybersecurity, the gap in oversight over data privacy is equally problematic. There is no doubt that consumers across the country would benefit from a far more comprehensive regulatory approach to these issues. Our regulatory institutions need to rapidly adapt to the challenges presented by social media giants, big tech, and the analytics industry, and it is imperative that we put in place a clear nationwide legal framework for accountability enforced by a robust federal regulator.

In the meantime, Governor Cuomo has proposed bold action in New York. The Governor's executive budget proposal includes a comprehensive data privacy law, the New York Data Accountability and Transparency Act ("NYDATA"), that would significantly enhance privacy protections for New Yorkers.[7] The law would mandate that any entity that collects data

[5] Federal Trade Commission Press Release, Developer of Popular Women's Fertility-Tracking App Settles FTC Allegations that It Misled Consumers About the Disclosure of their Health Data (Jan. 13, 2021).
[6] N.Y. Dep't of Fin. Servs, Twitter Investigation Report: Report on Investigation of Twitter's July 15, 2020 Cybersecurity Incident and the Implications for Election Security (Oct. 14, 2020).
[7] California has recently taken action on this front as well. On November 3, 2020, California voters passed Proposition 24, known as the California Privacy Rights Act of 2020 ("Prop 24"), a ballot measure regarding data privacy. Prop 24 expands certain provisions of the California Consumer Privacy Act ("CCPA"), which was passed

on large numbers of New Yorkers disclose the purposes of such collection, and limit the data collected to that purpose. Notably, NYDATA would expressly protect categories of sensitive information such as health, biometric and location data, as well as create strong enforcement mechanisms to hold entities accountable. The proposal would further establish a Consumer Data Privacy Bill of Rights, which would ensure that New York consumers have the legal right to access, control, and delete any data collected from them. As Governor Cuomo stated: "[i]n a world where we are reliant on technology to work, learn, and even see our family, New Yorkers deserve transparency and accountability from the companies who collect and use their information."[8] This investigation has shown that the NYDATA law is necessary.

in 2018, and establishes a California Privacy Protection Agency authorized to enforce the CCPA, which will go into effect in 2023. It further requires businesses not to share a consumer's personal information upon the consumer's request, provide an opportunity for consumers to opt-out of data sharing for advertising or marketing purposes, and obtain permission or parental permission before collecting data from consumers who are younger than 16 or younger than 13, respectively. L. Hautala, Proposition 24 Passes in California, Pushing Privacy Rights to the Forefront Again, CNET (Nov. 4, 2020).

[8] C. Siegal, Gov. Cuomo Announces Proposal to Safeguard Data Security Rights, NEWS10 (Jan. 18, 2021).

About The New York State Department of Financial Services

Governor Andrew M. Cuomo and the New York State Legislature created the Department in 2011 from the merger of the former Banking and Insurance Departments, and widened the Department's purview to include "the regulation of new financial services products" by establishing "a modern system of regulation, rulemaking and adjudication" responsive to the needs of New York consumers.

The Department is the primary regulator of a broad spectrum of financial services providers that operate in the State of New York, including state-chartered banks, foreign banks with branches in New York, insurance companies and their agents and brokers, non-depository lenders, money transmitters, and check cashers. The Department supervises and examines licensed entities, promulgates applicable regulations, and enforces the law through investigations and, where necessary, administrative proceedings.

Consumer protection is central to the Department's mission. Under the leadership of Superintendent Linda A. Lacewell, in 2019, the Department announced the creation of its Consumer Protection and Financial Enforcement Division ("CPFED") to "strengthen the Department's mandate to guard against financial crises and to protect consumers and markets from fraud." CPFED is responsible for protecting consumers, fighting consumer fraud, and ensuring that regulated entities comply with New Yok and federal law in relation to their activities serving the public, as well as enforcing New York's Banking, Insurance, and Financial Services Laws with a particular focus on the development of supervisory, regulatory, and enforcement policy in the area of financial crimes.