WELCOME to the inaugural issue of Jenner & Block’s Consumer Finance Observer or CFO! In this periodical newsletter, our lawyers from a broad range of practice areas provide analysis of key consumer finance issues currently on the minds of regulators, companies and practitioners. They update you on important developments to watch. You can also find regular consumer law updates by visiting our Consumer Law Round-Up at consumer.jenner.com.

District Court in New York Blocks FinTech Charter

Jeremy Creelan and William Goldstein

In early May, a federal district court in New York effectively blocked the Office of the Comptroller of the Currency (OCC) from issuing national bank charters to non-bank FinTech companies that do not receive deposits. The court denied the OCC’s motion to dismiss a suit brought by the New York Department of Financial Services (DFS), which argues that issuing charters to FinTech companies would deprive DFS of jurisdiction over such entities and correspondingly lead to the loss of “critical financial protections” for New Yorkers. Vullo v. Office of the Comptroller of the Currency, No. 18-cv-8377, 2019 WL 2057691, at *8 (S.D.N.Y. May 2, 2019). In denying the OCC’s motion, the court decided the central legal issue in DFS’s favor, holding that the National Bank Act unambiguously requires an institution to receive deposits in order to be in the “business of banking” and thus to be eligible (absent some statutory exception) for a national bank charter. Id. at *18. The court’s decision casts doubt on whether nationwide regulation of FinTech companies can be achieved without action by Congress. As of late June, the parties were negotiating the language of a proposed final judgment to submit to the court, presumably to allow for an appeal.

Jenner & Block
In May 2019, the Consumer Finance Protection Bureau (CFPB) addressed debt collection practices by announcing a long-awaited notice of the proposed Fair Debt Collection Practices Act (FDCPA) and ESIGN Act rulemaking that was authorized by Dodd-Frank. The proposed rulemaking represents the first meaningful regulation to issue into a space that has been a creature of periodic case law with at times divergent views.

The CFPB states that it does not intend to generally codify existing case law. When issuing the 500-plus page notice, the agency emphasized that the proposed rulemaking would establish some bright lines regarding limitations on call attempts and telephone conversations, and clarify required disclosures and how debt collectors can communicate with consumers. The CFPB also noted provisions to address time-barred debt and impose a prerequisite of communication with a consumer prior to a debt collector furnishing information about a debt to credit reporting agencies.

Less emphasis was placed on other important topics, such as whether the judicially created “least sophisticated consumer” standard will be employed under the FDCPA—the CFPB agrees with an “objective” standard and proposes the use of the term “unsophisticated” while citing “least sophisticated consumer” case law with approval. Also receiving less emphasis was a provision that “generally would prohibit a debt collector from selling, transferring or placing for collection a debt if the debt collector knows or should know that the debt has been paid or settled, discharged in bankruptcy, or that an identity theft report has been filed with respect to the debt.”

Undoubtedly the proposed rule will be closely examined by those who attempt to collect debts on behalf of others, and thus fit within the definition of a debt collector under the FDCPA. But the proposed rule may be of significant interest to those seeking payments upon debts owed to themselves. Indeed, financial institutions have looked to FDCPA case law as providing some practical guidance as to what collection behavior might run afoul of general principles of unfair or deceptive conduct—even before the CFPB’s 2013 guidance that originating creditors must refrain from unfair, deceptive and abusive acts or practices (UDAAP) when collecting their own debts. Thus, elements of the proposed rule, such as a cap of the number of calls per week and a cooling off period after an actual conversation, may be worthy of comment. Other elements of the proposed rule worthy of note include requiring opt-out instructions in every email and text to a consumer, a prohibition against using a work email address without prior consent and limitations on the use of social media platforms.

The comment period is open and any comments must be received by August 19, 2019.
The Saga of *Madden v. Midland Funding* Continues

Joseph Noga, Michael Ross and William Goldstein

In 2015, the Second Circuit made news in the marketplace lending industry—and the market for bank-originated debt more broadly—when it held, in *Madden v. Midland Funding*, LLC, that a non-bank purchaser of bank-originated credit card debt was subject to New York State’s usury laws. 786 F.3d 246, 250-51 (2d Cir. 2015). That widely discussed case continues to generate interest.

One notable element of *Madden* was that it did not address principles that lenders and debt purchasers had previously taken as given. Nationally chartered and FDIC-insured banks are exempt under federal law from various state and local regulations—including state usury limits that are lower than those of the bank’s home state. Most have understood that, when banks sell debt to third-parties, the purchasers can seek the entire balance of the loan, including amounts that were above the state usury cap when applied. That understanding is based largely on the “valid-when-made” principle, a concept under longstanding contract law that “an assignee stands in the shoes of the assignor, including when those shoes charge interest.” See Charles M. Horn & Melissa R. H. Hall, *The Curious Case of Madden v. Midland Funding and the Survival of the Valid-When-Made Doctrine*, 21 N.C. BANKING INST. 1, 6-7 (2017). Without addressing “valid-when-made,” however, *Madden* concluded that preemption did not apply to the third-party debt buyer.

Critics have zeroed in on the *Madden* court’s failure to consider “valid-when-made” (which the defendants did not brief). Some have emphasized the contractual nature of the doctrine, arguing that if the issuing bank validly exported its home-state interest rate to a third party, at that point “valid-when-made” should kick in as a matter of contract law and allow assignees to charge the original interest rate, with no need to invoke additional preemption principles beyond basic rate exportation. Horn & Hall, supra, at 13-21. Other critics—most notably the Solicitor General at the time of the petition for certiorari—have focused on the preemptive character of the doctrine, describing the court’s failure to consider “valid-when-made” not as overlooking a principle of contract law, but as a failure “to understand how application of state usury laws… would impair the bank’s exercise of [its] powers.” See OSG Brief at 12, 2016 WL 2997343, at *11-12. Most have highlighted the importance of rate-exportation to the functioning of credit markets. Regardless of how the doctrine is characterized, there is widespread criticism that the *Madden* court’s failure to consider the doctrine led it to an unwarranted result.

As of May of this year, no legislative or regulatory pronouncement on the issue seemed imminent. But a putative class action filed last month in the Eastern District of New York against non-bank defendants has the potential to address the issue. The complaint alleges that the New York usury cap applies to credit card debt that was pooled and sold in connection with a securitization. See Complaint, Cohen v. Capital One Funding, LLC, et al., 19-cv-03479 (E.D.N.Y. June 12, 2019). Because the debt is no longer held by the originating bank or a bank affiliate, the complaint says, New York’s usury limit is not preempted under *Madden* and is therefore usurious. The complaint does not discuss the “valid-when-made” doctrine, although most presume it will be raised by the non-bank defendants. Thus, the case has the potential to test the practical impact of *Madden*. Defendants’ answer—due August 19, 2019—will be one to watch.
News from the CFPB’s UDAAP Symposium

Kali Bracey

Under the Dodd-Frank Act, it is unlawful for any provider of consumer financial products or services to engage in any “unfair, deceptive or abusive act or practice” (UDAAP). On June 25, 2019, the CFPB gave its first symposium on whether the term “abusive” needs to be formally defined.

There were two panels of UDAAP experts at the symposium—one panel of academics and one panel of state attorneys general and practitioners. Thepredicate for discussion was that the term “abusiveness” has been less well developed than the terms “unfair” or “deceptive,” raising the issue—which the CFPB is formally considering—whether rulemaking or “other activities” may be helpful to further clarify its meaning. The panelists fell generally into two camps – those who believed that the Bureau needed to provide more clarity around the abusiveness standard and those who did not.

THOSE IN FAVOR OF A CLEAR DEFINITION

Those who were in favor of a definition listed the following reasons: uncertainty in the marketplace; lack of distinction between abusiveness, unfairness and deception; and stifling of innovation.

First, two professors argued for the need to provide clear definitions through rulemaking, not enforcement. Professor J. Howard Beales noted that the Bureau should tell both internal and external stakeholders what it cares about to alleviate uncertainty. Without limits, Beales stated, the staff is left to what he called Star Trek law enforcement: “go where no man has gone before.” Similarly, Professor Todd Zywicki noted that the Bureau needed to “build fences” to show what is in and what is out. For support, Professor Zywicki noted two instances of the enforcement and rulemaking parts of the Bureau defining abusiveness differently. He said that a clear definition could prevent these conflicts in the future.

Second, commentators noted that enforcement without a clear rule had left the definition muddled. Lucy Morris, a former enforcement lawyer at the Bureau, noted that enforcement cases have not distinguished between abusiveness and deception, and that because enforcement at the Bureau muddied the definitions within UDAAP, it is not clear where the lines are. According to Eric Mogilnicki, a lawyer in private practice, because the Bureau is not acting from a core set of principles, it is not clear why enforcement brings an abusiveness claim in one case and neglects to bring one in a case with similar facts.

Third, some panelists noted that the lack of certainty means that innovative products are not getting to the most vulnerable consumers. Given that abusive practices seem to be those targeting consumers who are less able to comprehend financial products, companies are reluctant to market to those consumers given the uncertainty in the law.

THOSE AGAINST A CLEAR DEFINITION

Those on the other side noted a variety of reasons a clearer definition was not yet needed.

First, those who were not in favor of a definition of abusiveness at this stage noted that the Federal Trade Commission (FTC) took 46 years to define unfairness and there was no need for the Bureau to rush here. Professor Patricia McCoy stated that the FTC took the time to allow the standard to develop on a case-by-case basis. Rather than a rule, she said, the Bureau can use no-action letters, guidance, and judicious use of enforcement and supervisory discretion. Moreover, according to Nick Smyth, a former CFPB enforcement lawyer who is now in the Pennsylvania State Attorney General’s Office, courts have not struggled with addressing abusiveness claims. In almost a dozen cases that courts have decided, they have been able to render an opinion without
looking to the legislative history. According to Professors McCoy and Smyth, the case law should be allowed to develop.

Second, several participants noted that the industry has been unspecific on how innovation is being inhibited or compliance costs increased simply by a lack of definition of the abusiveness standard. For instance, they said, no one can really imagine a product that is abusive but not unfair or deceptive, or can identify any compliance costs for abusive above and beyond those for unfair and deceptive. With respect to innovation, they pointed to a lack of evidence that firms have failed to extend or cut off credit as the result of a failure to define abusiveness. McCoy also pointed out that banks, FinTech companies and mortgage providers have not faced abusiveness claims. Rather, the focus has been on so-called fringe companies, and fringe products that target the most vulnerable consumers.

Third, panelists noted that the statute does not permit the Bureau to define abusiveness in a general way. For example, Smyth noted that according to 12 U.S.C. §5531(b): “The Bureau may prescribe rules applicable to a covered person or service provider identifying as unlawful unfair, deceptive, or abusive acts or practices in connection with any transaction with a consumer for a consumer financial product or service or the offering of a consumer financial product or service.” Because section §5531 specifies acts or practices, Smyth stated, the Bureau is not permitted to define abusiveness generally.

The symposium was the beginning of an information-gathering process and it does not appear that the CFPB is eager or prepared to define abusiveness anytime in the near future. CFPB Director Kathy Kraninger noted the symposium was the first in a series that will reflect diverse viewpoints and ideas to inform policy development. In the future, the CFPB hopes to address topics such as disparate impact and the Equal Credit Opportunity Act (ECOA), small businesses, cost-benefit analysis and consumer-authorized financial data sharing. The Bureau is aiming to have the next symposium in September.

---

**Crypto Corner – Updates on Cryptocurrency**

**Michael Ross**

In the first half of 2019, the “crypto-winter” that had set in during 2018 appeared to see signs of a thaw, albeit with new regulatory developments and controversy continuing to characterize the space. On the regulatory front, the Securities and Exchange Commission (SEC) issued more detailed guidelines for companies seeking to sell digital tokens. The 13-page “Framework for ‘Investment Contract’ Analysis of Digital Assets” provides a detailed analysis of the factors relevant to the Howey test that the SEC uses to determine the existence of a security (and all that designation entails). At the same time, the SEC issued a no-action letter for a company that had represented it would not be using its tokens to fund the development of the token network, and that the tokens would be immediately usable – underscoring two key factors of the SEC’s assessment. At the same time, the SEC issued a no-action letter for a company that had represented it would not be using its tokens to fund the development of the token network, and that the tokens would be immediately usable – underscoring two key factors of the SEC’s assessment. In another development, the Financial Action Task Force (FATF) – a global inter-governmental organization focused on fighting money-laundering – issued new guidelines on cryptocurrency companies operating in its 37 member countries, including requirements about collecting user information. FINRA has also decided to continue a reporting initiative it announced last year.

On the news-making front, much industry attention was paid to the SEC’s suit against a Canadian messaging company called Kik Interactive, alleging that Kik propped up its failing business by pivoting to an unregistered token offering through which it raised $100 million. Some have viewed the case as one to watch to see whether courts will view digital tokens the same way as the SEC has. More recently, focus on developments at the SEC have been overtaken by news of Facebook’s anticipated Libra token. Built on a permissioned blockchain network overseen by a litany of household names, and backed by a basket of traditional assets, the Libra token met early news of its potential to change the game for cryptocurrency. More recent weeks have seen a flurry of commentary by regulators and legislators focused on the need to analyze the token under existing financial services laws, as well as concerns about money-laundering, consumer protection and privacy. For those interested in the space, it will be worth monitoring further developments as they unfold.
The FDIC’s Consumer Compliance Supervisory Highlights

Damon Smith

Last month, the Federal Deposit Insurance Corporation (FDIC) issued its first Consumer Compliance Supervisory HIGHLIGHTS publication. The FDIC said that the publication is designed to document their consumer compliance supervision activities for 2018, and to provide a “high-level overview of consumer compliance issues identified during the year.”

Overall, the FDIC’s approximately 1,200 risk-based consumer compliance examinations rated 98 percent of supervised institutions satisfactory or better for consumer compliance. Of the two percent that rated as less than satisfactory, the most commonly reported weakness was in their overall compliance management systems (CMS). The FDIC highlighted specific issues in the following areas:

- **OVERDRAFT PROGRAMS** – the use of inadequately disclosed balance calculation methods that could result in double-counting overdrafts where a point-of-sale (POS) transaction is authorized and settled at two different times;

- **REAL ESTATE SETTLEMENT PROCEDURES ACT (RESPA)** – Section 8 violations arising from evasions of RESPA’s anti-kickback provisions including kickbacks disguised as above-market payments for office/desk rentals or marketing agreements;

- **THE ELECTRONIC FUND TRANSFER ACT (EFTA, OR REGULATION E)** – failure to properly calculate the 60-day refund rule from the date when a consumer is provided notification of transactions; failure to investigate promptly when notified of errors; failure to provide notice of investigation completion and discouraging filing of error resolution requests by requiring branch visits, notarized affidavits, police reports or requiring agreement to assist law enforcement and court activities;

- **SKIP-A-PAYMENT LOAN PROGRAMS** – inadequate disclosures of program terms and impacts and assessing late fees for skipped payments under the program; and

- **LINES OF CREDIT FINANCE CHARGE CALCULATIONS AND DISCLOSURES** – inaccurate calculations and disclosure of finance charges or annual percentage rates (APRs) on periodic statements.

In addition to those highlighted issues, the FDIC reported that the most frequently cited violations were:

- The Truth in Lending Act (Regulation Z) with two level 3 violations and 322 level 2 violations;

- Truth in Savings Act (Regulations DD) with five level 3 violations and 135 level 2 violations; and

- EFTA/Regulation E with three level 3 violations and 123 level 2 violations.

The piece also contained a few “best practices” to avoid common compliance issues and links to FDIC resources and information for regulated financial institutions. As an initial publication, HIGHLIGHTS provided a helpful but very broad overview of the FDIC’s supervisory findings. It will be interesting to see if additional detail and guidance will be provided in future issues.

Texas Enacts New Consumer Finance Laws

Joseph Noga

Texas recently added to governmental efforts to address perceived issues concerning time-barred debt by enacting into law a provision that precludes a “debt buyer” from commencing an action or initiating an arbitration against a consumer to collect a consumer debt after the expiration of the applicable Texas statute of limitations period. See H.B. No. 996. The statute also makes clear that there can be no revival of the debt caused by any activity on the consumer debt, including reaffirmation. The statute does not preclude attempts to collect debt past the statute of limitations entirely, however, although it does have a mandatory disclosure scheme in which the disclosure provision to be used is dependent upon whether information about the debt is being furnished, or can be furnished in compliance with the FCRA’s limited seven-year reporting period from date of first delinquency. The overwhelming support for the bill is notable. The Senate passed the bill 31-0 and the House 133-7. The statute takes effect September 1, 2019.
Everyone is focused on how companies are using the customer data they collect. Headlines call out changes to privacy rules in Europe, California, and elsewhere, and consumers regularly receive notifications of massive data breaches. With all this going on, there is another piece of the data puzzle that companies need to be talking about and preparing for: the wave of enforcement activity that has begun to focus on how companies are using the sensitive data they collect in making business decisions – to approve or deny a loan, to target an advertisement, or to pick a neighborhood for offering a new service.

With this wave of activity, and more likely to come, any business that uses sensitive data as part of its decision making needs to remain focused on more than the rules for how to safeguard sensitive customer data; it must also stay informed about the enforcement actions being taken by regulators throughout the country about how companies use that data to make business decisions. This article addresses three key areas of interest for regulators: discrimination and unfairness; accuracy; and security and transparency.

ENFORCEMENT AUTHORITIES ZEROING IN ON ALTERNATIVE DATA

David Bitkower, Kali Bracey, Jeremy Creelan, Joseph Noga and Michael Ross
DATA USAGE ON THE REGULATOR BRAIN

In recent years, regulators have signaled to the public an increasing concern over the way that companies may be using data about their clients and customers, particularly when it comes to making financial decisions like extending credit. For example, the FTC – which has jurisdiction over consumer protection and competition in commerce – has held multiple hearings over the past several years about the intersection of “big data” and consumer protection. Those hearings have focused in part on the concern that using big data in commerce can lead to discrimination and privacy concerns. In 2017, the CFPB issued a request for information noting that using alternative, non-FICO data for credit decisions raises regulatory concerns. In 2018, more than 25 state attorneys general submitted comment to the FTC raising consumer welfare concerns regarding use of algorithmic decision tools, artificial intelligence (AI) and predictive analytics. These are just a few examples of government authorities becoming more focused on how companies are using the data they collect.

REGULATION THROUGH ENFORCEMENT

Numerous regulators have authority under existing laws to take action against companies that adversely affect consumers. Most broadly, the FTC Act prohibits “unfair or deceptive acts or practices in or affecting commerce.” A practice can be unfair, for example, if it “causes or is likely to cause substantial injury to consumers” that is not outweighed by any countervailing benefits to consumers and that consumers themselves could not reasonably have avoided.” Another provision of federal law enables the CFPB to enforce a prohibition against businesses engaging in “unfair, deceptive, or abusive acts or practices” – the so-called UDAAP authority (discussed further in an article on page 4). And most states have similar provisions that government or private parties can enforce. In short, various existing laws provide broadly-worded grants of power to regulators to pursue an enforcement action against consumer-facing activity they deem undesirable. The breadth of the standards, coupled with the variety of enforcement authorities, can make it difficult to predict what practices will fall under regulatory scrutiny.

DISCRIMINATION AND UNFAIRNESS

It is well established law that companies cannot make business decisions – particularly credit decisions – that discriminate on the basis of a protected characteristic, such as race, gender, religion or country of origin. But what happens when a company employs a decision-making algorithm that does not expressly use race, but uses another factor that ends up serving as a proxy for race? That too can constitute discrimination. For example the FTC has said that using zip codes in a decision can be an unlawful proxy for a race-based decision and could therefore constitute an “unfair” practice under the FTC Act. And what about more complex algorithms that use machine learning or nuanced AI to cull data to find correlations that are then used to make decisions on who is credit-worthy and who is not? For example, crunching available data may show that members of a particular group are more likely to default on loans or apply for less attractive credit products. The FTC has also said that a company could face potential liability for targeting its advertising for only those less attractive products to that group, if it leads to members of the protected group obtaining only those less attractive products. And in its June 28, 2019, Fair Lending Report, the CFPB noted that “[t]he use of alternative data and modeling techniques may expand access to credit or lower credit cost and, at the same time, present fair lending risks.” The agency recommended supervisory reviews of credit-scoring models, and also noted as an area of enforcement focus the use of models to predict recovery outcomes in collecting credit card and auto loan debts.

Two recent examples show how using data analytics to target consumer marketing needs to be approached with particular sensitivity. In one well-publicized example, Amazon failed to offer same-day delivery service to certain minority neighborhoods in New York and other cities. Following claims that Amazon was using geography as proxy for race, a US congressperson sent a letter to the FTC, arguing that Amazon’s conduct might be an “unfair” business practice under the FTC Act and violation of the Civil Rights Act of 1964. Amazon quickly expanded its same-day delivery service to those neighborhoods to calm the uproar. In another example, the US Department of Housing and Urban Development (HUD) filed a charge of discrimination against Facebook, alleging the company violated the Fair Housing Act (FHA) “by encouraging, enabling, and causing
housing discrimination through the company’s advertising platform.” Other enforcement actions have focused on the use of data about a customer’s source of income (e.g., child support payments) in a credit decision, or targeting loan advertisement to neighborhoods that did not have high numbers of Black or Hispanic residents.

As these examples indicate, enforcement authorities will expect companies not to use their data analytics to make decisions that – whether they know it or not – end up targeting or excluding particular consumer groups, or that have a disparate impact on those groups, in a manner that can be considered unfair or discriminatory. Thus, companies ought to be on the lookout to ensure they understand the data inputs that are driving decisions; and, as importantly, they need to understand the business reasons they are making decisions, beyond the mere the fact that the data has shown a correlation. In other words, just because a data set shows a particular correlation that may not necessarily provide a justification on its own for a decision that could later be challenged. As a practical matter, it will likely be important for companies to consider including a human element to in their assessment process—to look at the input and the outputs, and to look out for correlations that may, even unwittingly, serve as a proxy for a protected characteristic. Critical human input can help guard against employing a process that ends up having unintended, problematic consequences.

**ACCURACY**

Another key, albeit more nascent, area of regulatory concern is the accuracy of alternative data that a company acquires, uses or sells for use in decisions about consumers. After a honeymoon period—where the focus has been the benefits of alternative data with respect to reaching no or thin-file consumers outside the traditional credit system and disrupting the big three credit reporting agencies—consumer advocates and governmental authorities are beginning to question how information is being collected and characterized, and whether it is utilized in a manner consistent with the real-world facts.

The Fair Credit Reporting Act (FCRA) has long-provided a framework for assessing the accuracy of traditional consumer credit information. The FCRA provides a basis for consumer reporting agencies (CRAs) to reasonably rely upon sources of information, subject to providing consumers with an opportunity to review and correct the information. It further places certain obligations upon those who furnish information to the reporting agencies and those who obtain information about consumers from them. By contrast, alternative data is sometimes defined as anything that does not fall within the traditional buckets of information obtained and used by the CRAs. Thus, for those whose operations have a nexus to alternative data, a threshold question is whether they or anyone with whom they are interacting falls within the definition of a CRA and what obligations are imposed if they do. The uninitiated often find the definitions are not intuitive.

Additionally, there is the beginning of a focus on alternative data falling outside the FCRA regulatory scheme. The US Government Accountability Office (GAO) reported in December 2018 that the CFPB and federal banking regulators are monitoring use of alternative data by collecting information and developing reports, but have not provided specific guidance on using the data. The reliability of data was deemed one of the risks and the GAO called upon multiple federal agencies to address the appropriate use of alternative data in underwriting. For its part, the CFPB “commit[ted] to providing information in the future on alternative data” and in the CFPB’s Fair Lending Report mentioned above stated that a “significant focus” of the Bureau is going to be how credit decisioning models use alternative data. The National Consumer Law Center recently issued a paper that included a warning about errors and inaccuracies in alternative data and the inability to correct them.

Recent FTC enforcement activity has also focused on third-party data. The FTC has settled enforcement cases with data brokers that have failed to give consumers an opportunity to correct erroneous data and for employing dispute resolution procedures that made the correction process particularly burdensome for the consumer. Enforcement has also focused on the failure to provide users of data with notice of when such third-party data was used to adversely affect a credit or other similar decision. Thus, companies selling or using third-party data in relevant consumer decisions should consider whether they have sufficient processes in place to permit user feedback for data, and that they engage in periodic data reviews to assess the completeness or accuracy of their data.

**TRANSPARENCY**

The security of consumer data is another key issue for businesses, and keeping up with the rules of numerous government authorities is of paramount importance. But broad enforcement action by consumer protection regulators is also an important aspect of this area to have in mind.

In the leading case of *FTC v. Wyndam Worldwide Corporation*, the FTC brought an action against the hotel company for failing to adequately safeguard consumer information and for misstating its security practices to those consumers. In that action, the FTC charged that such conduct amounted to unfair or deceptive acts or practices under the FTC Act. Since then the FTC has brought numerous other actions, including against tech companies, under the same basic theory. Expanding its reach, the FTC has focused on third-party data. The FTC has also more recently initiated enforcement actions against tech companies that have not adequately disclosed to consumers the kinds of data they were collecting from them on their platform, as well as other similar theories. As noted above, numerous state regulators have similar authority under parallel state law regimes.

With this area of increasing interest to regulators, it may be expected for regulators using broadly-worded enforcement authority to act in still-uncharted areas in which companies are collecting and using various types of sensitive and
personal data. Enforcement activity targeting data use that regulators might deem “unfair” could include areas such as facial recognition or automated data collection of repeat, high-volume activities. As these practices become more common, companies should consider conducting periodic audits of data collection and use that involve a cross-section of organizational stakeholders, limiting data collection to what is needed, periodically re-vetting consumer disclosures, and keeping updated with both regulator guidance and enforcement activity.

CONCLUSION
As data use becomes increasingly key to businesses – and regulators – companies must do more than get up to speed on the basic privacy and data security rules. Enforcement authorities have already laid the groundwork for focusing their attention on whether the ways companies use data can be considered unfair, deceptive, or abusive in some way. An existing body of regulatory activity, detailed above, can help guide the way toward the kinds of activities we already know are of interest to government actors – particularly their concern for discrimination, accuracy, and transparency. And, as regulators try to keep up with the developments in the way companies are using data, companies are themselves well advised to keep up on enforcement activity by regulators.

This article was first published by Law360 on July 23, 2019.