A New Era of Federal Trade Commission ("FTC") Privacy and Cybersecurity Oversight: Top Ten Things Companies Should Know When Assessing FTC Compliance and Exposure

January 12, 2022

Companies developing FTC compliance programs, or under investigation by the FTC's Bureau of Consumer Protection, should be aware of significant developments impacting the Commission's regulatory authority and enforcement priorities.

Despite a number of recent judicial defeats that have significantly hampered the FTC's ability to obtain: (1) injunctive relief when purported violative behavior is not ongoing; and (2) monetary remedies in federal court under Section 13(b) of the Federal Trade Commission Act (the "FTCA"), new FTC Chair Lina Khan has indicated that the FTC intends to aggressively enforce existing FTC consumer protection laws—and in particular alleged privacy and cybersecurity violations.

The aggressive nature of the FTC under Chair Khan has its critics. The two Republican commissioners have expressed disagreement with the Democratic majority regarding the breadth of the FTC's existing legal authority and have recently issued a number of strongly worded dissents.[1] Although the FTC is typically not overly political, and is often apolitical, in this instance there appears to be a significant difference in regulatory philosophy that may impact the functioning of a divided FTC.[2]

Based upon these developments, companies subject to privacy and cybersecurity enforcement by the FTC should be cognizant of a number of judicial, regulatory, and legislative crosscurrents that impact the FTC's investigative approach and enforcement

---

1 *E.g.*, Dissenting Statement of Commissioners Christine S. Wilson and Noah Joshua Phillips Regarding the Commission Statement on the Adoption of Revised Section 18 Rulemaking Procedures (July 9, 2021); Dissenting Statement of Commissioner Noah Joshua Phillips Regarding the Report to Congress on Privacy and Security (Oct. 1, 2021); Statement of Commissioner Christine S. Wilson Concurring in Part and Dissenting in Part Regarding the Report to Congress on Privacy and Security (Oct. 1, 2021).

2 As of the writing of this article, based upon the recent departure of one of the Democratic Commissioners (Rohit Chopra, who was confirmed as Commissioner of the Consumer Financial Protection Bureau (the "CFPB")), the FTC has only four commissioners: two Republican and two Democratic. President Biden, however, nominated privacy expert Alvado Bedoya on September 13, 2021, to be the fifth commissioner, and the Democrats will again have a 3-2 majority if he is confirmed by the Senate.

authority. This article provides an overview of ten key points companies should be aware of when developing FTC compliance programs, remediating past behavior, or confronting FTC privacy or cybersecurity enforcement. Although this article focuses on privacy and cybersecurity compliance, many of the issues described below apply equally to advertising and marketing practices that may also result in FTC scrutiny.

1. Monitor Aggressive Policy Developments under New FTC Chair Lina Khan

As noted in a prior Debevoise in Depth article, on July 1, 2021, the FTC implemented a number of rules and policies that signal the arrival of a new era of aggressive FTC enforcement.[3] In fact, possibly anticipating an immediate need for additional personnel to implement its enforcement agenda, the FTC reportedly ordered staff to cancel all public appearances and issued a moratorium on public events and press outreach. This was followed by President Biden's July 9, 2021, Executive Order on "Promoting Competition in the American Economy" that further empowers the FTC to more aggressively apply its legal authorities, targeting a number of industry sectors including healthcare (particularly hospitals, health insurers, and companies selling prescription drugs and hearing aids) and technology.[4]

Shortly after Chair Khan's confirmation, with only one week's notice to their two Republican colleagues, the three Democratic commissioners voted to implement dramatic changes to a number of FTC rules and policies including a new rule governing "Made in USA" claims ("MUSA claims") and changes to the traditional Magnuson-Moss rulemaking procedure that could expedite future rulemaking efforts—particularly targeting privacy, cybersecurity and other priorities outlined in the President's July 9 Executive Order.[5]

In a motion passing 3-2 on a party-line vote, the Democratic commissioners removed the Chief Administrative Law Judge (the "ALJ") from the role of Presiding Officer in Magnuson-Moss rulemaking; Chair Khan or her designee will instead assume the role of Presiding Officer, giving Chair Khan even greater control over future rulemaking efforts.[6] The motion also removed the requirement to have a staff report accompany all

---

3 Debevoise in Depth: Flurry of New FTC Rules and Policies Signals Era of Aggressive Enforcement Despite Recent Supreme Court Defeat (July 13, 2021).

4 Executive Order on Promoting Competition in the American Economy (July 9, 2021).

5 On June 23, 2021, Republican FTC Commissioner Christine Wilson signaled that despite significant reservations, she is now prepared to join with her fellow Democratic commissioners to authorize promulgation of an FTC privacy rule.

6 FTC Press Release, Statement of Commissioner Rebecca Kelly Slaughter Joined by Chair Lina Khan and Commissioner Rohit Chopra: Regarding the Adoption of Revised Section 18 Rulemaking Procedures (July 1, 2021).

rule recommendations. The dissenting Republican commissioners argued that these changes both threaten the independence of FTC rulemaking and lend legitimacy to public criticisms that the FTC is a politically motivated agency—increasing the risk of congressional backlash.[7]

Subsequently, on September 22, 2021, FTC Chair Khan issued a memo to fellow FTC commissioners and Commission staff entitled: "Vision and Priorities for the FTC."[8] The memo describes a new strategic vision for the FTC in a period of change and transformation. Among other things, the Commission expects to take a holistic approach to enforcement focusing on "root causes" rather than one-off effects.

Recent FTC statements specifically address the Commission's aggressive focus on privacy and cybersecurity enforcement. On September 13, 2021, the FTC issued a controversial 36-page report to Congress titled "FTC Report to Congress on Privacy and Security."[9] The report establishes privacy and cybersecurity enforcement as a priority for the FTC and requests additional funding from Congress to support the FTC's efforts. The report describes the following four areas of focus in the coming years: "integrating competition concerns, advancing remedies, focusing on digital platforms, and expanding on our guidance on and understanding of the consumer protection and competition implications of algorithms."[10] The FTC also appended a "statement" by Chair Khan explaining that "[p]olicing data privacy and security is now a mainstay of the FTC's work" and noting the frequent overlap between data privacy and competition.[11] The two Republican commissioners, however, issued strongly worded dissents questioning whether certain proposed FTC practices described in the report exceed the FTC's statutory authority.[12]

In addition, although the FTC's authority is limited to civil enforcement, on November 18, 2021, the FTC voted to expand its criminal referral program and issued a policy statement outlining new measures to combat criminal misconduct by corporations and their executives uncovered during FTC investigations. These new measures include public reporting on the FTC's criminal referral efforts on a regular basis, the development of guidelines for referrals and regular meetings with federal, state, and local criminal authorities to facilitate coordination.

---

7 Dissenting Statement of Commissioners Christine S. Wilson and Noah Joshua Phillips Regarding the Commission Statement on the Adoption of Revised Section 18 Rulemaking Procedures (July 9, 2021).

8 Memorandum from Chair Lina M. Khan, Vision and Priorities for the FTC (Sept. 22, 2021).

9 FTC Report to Congress on Privacy and Security (Sept. 13, 2021).

10 *Id.* at 3.

11 Statement of Chair Lina M. Khan Regarding the Report to Congress on Privacy and Security (Oct. 1, 2021).

12 *See* Dissenting Statement of Commissioner Noah Joshua Phillips Regarding the Report to Congress on Privacy and Security (Oct. 1. 2021); Statement of Commissioner Christine S. Wilson Concurring in Part and Dissenting in Part Regarding the Report to Congress on Privacy and Security (Oct. 1, 2021).

More recently, on January 4, 2022, the FTC issued an advisory informing companies of their obligation to remediate the Log4j security vulnerability and more generally ensure that security vulnerabilities are appropriately remediated.[13]

2. Monitor the FTC Commissioner Roster

With the recent departure of Rohit Chopra to lead the CFPB, there are currently only four commissioners (evenly divided between Democrats and Republicans). Last month, however, President Biden nominated privacy expert Alvaro Bedoya as FTC Commissioner. Bedoya is a Democrat, and, if confirmed by the Senate the Commission would again have a Democratic majority. Bedoya is currently a professor at Georgetown Law specializing in privacy law. He founded the school's Center on Privacy & Technology in 2014 and was previously chief counsel to the Senate Judiciary Subcommittee on Privacy, Technology and the Law. In that position, he helped organize oversight hearings on mobile location tracking and biometric privacy. He also wrote a well-known law review article titled "Privacy as a Civil Right."[14]

Although most FTC decisions are apolitical and unanimous, based upon the number of recent dissents by the Republican commissioners, there may be situations where FTC enforcement and policy directives may be constrained while the Commission does not have a Democratic majority. In order to avoid this outcome, the FTC under Chair Khan obtained a number of "zombie votes" from Commissioner Chopra immediately prior to his departure that would be "counted" even after his departure and until a new Commissioner is confirmed. In fact, the FTC enacted a new antitrust policy on prior approval provisions in merger orders by relying on a Chopra "zombie vote," despite strong dissents by the two Republican commissioners.[15]

3. Understand the FTC Civil Investigative Demand Process and Timelines

Many FTC consumer protection investigations (particularly for advertising violations) are initiated by FTC staff via informal "access letters." As a general rule, however, the FTC's Division of Privacy and Identity Protection (the "DPIP") initiates privacy and cybersecurity investigations via civil investigative demands ("CIDs"). A CID is a type of Commissioner-authorized subpoena, enforceable in court, that subjects the recipient to

---

13 Regulatory Risks of the Log4j Vulnerability: FTC Warns Companies to Take Reasonable Steps to Protect Consumer Data, Debevoise Data Blog (Jan. 7, 2022).

14 Alvaro Bedoya, Privacy as Civil Right, New Mexico Law Review, Vol. 50, No. 3 (May 12, 2020).

15 Dissenting Statement of Commissioners Christine S. Wilson and Noah Joshua Phillips Regarding the Statement of the Commission on Use of Prior Approval Provisions in Merger Orders (Oct. 29, 2021).

a number of formalized processes and timelines. Companies should be aware of the rules and procedures that govern the formalized CID process.[16] As a general rule, CIDs are confidential and not publicly disclosed by the FTC during the investigation period unless the recipient voluntarily discloses the existence of the investigation or files a petition to quash.

After reviewing the CID, a critical first step is the "meet and confer" with FTC staff, which must take place within 14 days after receipt of the CID. This is when critical subjects are discussed, including the potential for a rolling production and approaches to minimize the burden of the production. If disagreements remain, companies have the option of filing a petition to quash within 20 days after receipt of the CID. Such petitions are rarely successful and the petition and FTC response are publicly disclosed (which means the existence of the CID would become public).

4. Understand the FTC's Legal Standards for Establishing Deception or Unfairness

Section 5 of the FTCA prohibits unfair or deceptive acts or practices. Privacy and cybersecurity cases can be predicated on deception, unfairness, or both.

For cases predicated on deception, the FTC's "Deception Policy Statement" provides an overview of the Commission's authority.[17] As a general rule, there must be a material representation, omission, or practice that is likely to mislead reasonable consumers.

For cases predicated on unfairness, the FTC may consider an act or practice is unfair if it: (1) causes or is likely to cause substantial injury to consumers; (2) is not reasonably avoidable by consumers themselves; and (3) is not outweighed by countervailing benefits to consumers or to competition. FTC precedent suggests that "substantial" injury should implicate more than theoretical harm and should involve some form of tangible injury.

5. Evaluate Whether the Alleged Deceptive or Unfair Practices Are Ongoing

On February 25, 2019, the United States Court of Appeals for the Third Circuit upset decades of FTC practice by significantly limiting when the FTC can bring competition and consumer protection enforcement actions in federal court.[18] In *FTC v. Shire*

---

16 16 C.F.R. Part 2.

17 FTC Policy Statement on Deception (Oct. 14, 1983).

18 *See* Debevoise Update: The Third Circuit Sharply Curtails the FTC's Preferred Enforcement Power (Mar. 1, 2019).

ViroPharma, Inc., the Third Circuit ruled that absent an allegation that a violation of the FTCA "is" occurring or "is about to" occur, the FTC is limited to its administrative enforcement mechanism. This means that the FTC largely has lost its ability to seek injunctive and monetary relief for past violations that are not ongoing in Delaware, New Jersey, Pennsylvania, and the Virgin Islands. The decision could impact other Circuits as well.

The FTC is lobbying Congress to restore its ability to bring actions in federal court even if conduct is no longer ongoing or impending when the suit is filed and requested this legislative fix in its September 2021 Report to Congress.[19]

6. Recognize That the FTC Can Pursue Individual Liability under Certain Circumstances

Companies under investigation should be aware that the FTC can name individuals in its enforcement actions in addition to the company as a whole. To establish individual liability, the FTC must show that the individual defendant participated directly in the illegal practices or had authority to control them. The FTC will often consider whether there is a "culture of compliance" and if senior executives ignored warning signs. The FTC's goal in pursuing individual liability is to achieve specific and general deterrence and obtain appropriate injunctive relief. In this regard, one commissioner has noted:

> "In considering whether naming senior leaders is necessary for a settlement to achieve specific and general deterrence, I am particularly interested not only in the evidence of the leaders' involvement and knowledge but also in the extent to which the alleged law violations permeated a core aspect of the business and whether the corporate culture is one of compliance."[20]

Notably, individuals in large publicly traded companies are rarely named with respect to initial violations under the theory decision-making is diffuse at these large companies. Individuals in smaller companies, particularly active executives involved in day-to-day decision-making, are more likely to be named. The FTC even recently imposed individual liability on in-house counsel, but one Commissioner emphasized that the attorney was named based upon his actions while functioning in a business capacity rather than as an attorney.[21]

---

[19] FTC Report to Congress on Privacy and Security at 5 (Sept. 13, 2021).

[20] Dissenting Statement of Commissioner Rebecca Kelly Slaughter Regarding *FTC v. Progressive Leasing* (Apr. 20, 2020).

[21] Concurring Statement of Commissioner Christine S. Wilson, FTC v. ITMedia Solutions (Dec. 16, 2021).

7. Recognize the Importance of the Supreme Court's Recent *AMG Capital* Decision and the Potential Impact on the FTC's Ability to Obtain Monetary Remedies

Reversing decades of FTC precedent, on April 22, 2021, the Supreme Court in *AMG Capital Management, LLC v. FTC* unanimously held that Section 13(b) of the FTCA does not grant the FTC authority to obtain monetary remedies in federal court. The Supreme Court's decision overturned long-standing FTC reliance on Section 13(b) for monetary remedies and has far-reaching implications for pending and future FTC consumer protection and antitrust disputes.[22]

Although the plain language of Section 13(b) is limited to permanent injunctions, ever since the provision was enacted in 1973 the FTC has steadily expanded the use of Section 13(b) to seek monetary equitable remedies in consumer protection and antitrust cases. The FTC has obtained a wide range of equitable remedies under Section 13(b) including billions of dollars in monetary remedies (*i.e.*, restitution or disgorgement to compensate consumers for alleged harm arising from unfair and deceptive acts and practices found to violate Section 5 of the FTCA).

As a consequence of the AMG Capital decision, as described in greater detail immediately below, the FTC is likely to rely more heavily on administrative actions under Section 19 of the FTCA in lieu of initial proceedings in federal court. If the Commission issues a final administrative cease-and-desist order, the FTC may then bring a subsequent federal court case to obtain monetary remedies, though it would face a heightened standard of proof requiring evidence of "dishonest or fraudulent" conduct.

8. Understand the FTC's Administrative and Judicial Enforcement Options to Obtain Monetary Remedies despite the Supreme Court *AMG Capital* Decision

As explained below, the FTC is asking Congress to enact legislation that would in effect reverse the Supreme Court's *AMG Capital* decision and permit the agency to obtain monetary remedies under Section 13(b). In the absence of such legislation, however, the FTC has indicated that it intends to rely on other statutory provisions to obtain monetary remedies from companies accused of violating the FTCA.[23]

---

[22] *See* Debevoise In Depth: Unanimous Supreme Court Curtails the Federal Trade Commission's Authority to Obtain Monetary Remedies in Federal Court (Apr. 26, 2021); Debevoise Update: Third Circuit Strikes Another Blow Against the FTC's Preferred Enforcement Power, Setting the Stage for a Supreme Court Showdown (Oct. 5, 2020).

[23] The FTC has broader authority to obtain injunctive relief than monetary relief. Although the FTC's injunctive authority is not addressed in this article in any detail, we note that, in the privacy and cybersecurity context, the

Before addressing the primary mechanisms currently available for the FTC to obtain monetary remedies, it is important to distinguish between civil penalties and consumer redress. Civil penalties, which are paid to the U.S. Treasury, are based upon the number of violations of the FTCA and are not necessarily commensurate with consumer harm.[24] The maximum civil penalty amount is currently $46,517 per violation.[25] There is significant dispute regarding what constitutes a "violation," but the FTC generally takes the position that each consumer impacted by violative conduct constitutes a separate "violation." Consumer redress, on the other hand, refers to restitution or disgorgement that is tied to consumer harm (or the benefit obtained by a company allegedly violating the FTCA).

With that background, we summarize below the primary mechanisms the FTC can currently employ to obtain monetary remedies (*i.e.*, civil penalties or consumer redress) for consumer protection violations, including cybersecurity and privacy investigations:

- Civil Penalties[26] for Order Violations. Section 5(l) of the FTCA authorizes the FTC to obtain civil penalties against companies or individuals that are violating an existing FTC order against them. This provision is irrelevant for first-time offenders not subject to an existing FTC order or decree.

- Civil Penalties for Rule Violations. Section 5(m)(1)(A) of the FTCA authorizes the FTC to obtain civil penalties against companies or individuals who violate existing FTC rules. At the present time, however, there are limited FTC rules (due in part to the complex rulemaking process imposed by Congress) that would authorize civil penalties.[27] Examples include the telemarketing sales rule, children's online privacy

---

FTC has used its injunctive authority quite liberally, and companies can benefit from assessing prior cybersecurity/privacy FTC settlements in order to obtain insight into the breadth of the FTC's purported authority as well as guidance for developing compliance programs.

[24] The FTC must first refer civil penalty cases to the Justice Department pursuant to Section 16 of the FTCA. The Justice Department will decide whether to pursue the case and, if not, in most cases, the FTC can litigate on its own behalf. Companies targeted for civil penalty cases may have a jury trial.

[25] On January 6, 2022, the FTC published its updated inflation-adjusted civil penalty amounts, increasing civil penalties from $43,792 to $46,517 per violation. FTC Publishes Inflation-Adjusted Civil Penalty Amounts for 2022 (Jan. 6, 2022).

[26] The FTC's civil penalty authority was addressed by the Government Accountability Office (the "GAO") in January 2019. GAO, Internet Privacy: Additional Federal Authority Could Enhance Consumer Protection and Provide Flexibility (Jan. 2019).

[27] The FTC Safeguards Rule – which provides specific criteria for what safeguards nonbanking financial institutions, such as mortgage brokers, motor vehicle dealers and payday lenders, should implement to keep their customers' information safe – is an instructive example. *See* Debevoise Update, The FTC's Strengthened Safeguards Rule and the Evolving Landscape of Reasonable Data Security (Nov. 18, 2021). Although the FTC and U.S. GAO have historically indicated that the FTC does not have the authority to obtain civil penalties for violations of the FTC Safeguards Rule, it is unclear whether the FTC under Chair Khan will attempt to assert civil penalty authority. *See* GAO, Consumer Data Protection: Actions Needed to Strengthen Oversight of Consumer Reporting Agencies (March 26, 2019) ("However, FTC does not have civil penalty authority for

protection rule, and health breach notification rule.[28] In addition, the FTC is currently contemplating the issuance of a privacy/cybersecurity rule, but even if the agency goes forward with this initiative, it would take a number of years before such a rule would be finalized. In order to bring an action under this provision, the FTC must establish that the defendant had actual or constructive knowledge (*i.e.*, "actual knowledge or knowledge fairly implied on the basis of objective circumstances that such act is unfair or deceptive and is prohibited by such rule."). The FTC is also authorized to obtain consumer redress for rule violations (see below).

- Civil Penalties under the FTC's "Penalty Offense Authority." Section 5(m)(1)(b) of the FTCA contains a unique provision that under certain circumstances enables the FTC to obtain civil penalties from companies that knowingly engage in actions that have been previously deemed unfair or deceptive by the FTC and further documented in an order against a third party. These are challenging cases for the FTC to bring as the FTC must establish that the defendant had "actual knowledge that such act or practice is unfair or deceptive and is unlawful." Chair Khan has indicated that she intends to aggressively use this existing statutory provision, and in order to satisfy the "actual knowledge" requirement has had the FTC send letters to hundreds of companies purportedly putting them on notice that certain actions may result in civil penalties pursuant to the FTC's "penalty offense authority." Specifically, the FTC sent hundreds of letters to advertisers[29] (informing them of requirements applicable to testimonials and endorsements) and for-profit colleges[30] (informing them of prohibitions on certain types of false or deceptive claims) in an effort to better position the FTC to bring future civil penalty actions.

- Redress Actions for Rule Violations. Section 19(a) of the FTCA authorizes the FTC to obtain consumer redress in federal court for companies violating existing FTC

---

violations of requirements under the Gramm-Leach-Bliley Act (the "GLBA")…."); FTC v. RCG Advances LLC et al., FTC's First Amended Complaint for Civil Penalties, Permanent Injunction, Monetary Relief, and Other Relief (filed June 10, 2021); *see also* Proposed Rule: Standards for Safeguarding Customer Information, 84 FR 13158 at FN 123 (Apr. 4, 2019) ("A federal standard under GLB would be largely redundant because of state breach notification laws and because a requirement under the Rule would have limited effect, because the Commission cannot obtain civil penalties for violations of the Rule.").

[28] It is important to note that statutes other than the FTCA authorize civil penalties in certain circumstances. For example, the American Recovery and Reinvestment Act of 2009 instructed the FTC to issue a final rule requiring vendors of personal health records and mobile apps that interact with such records to notify consumers when the security of their data is compromised and authorized civil penalties for violations. The FTC has never enforced its Health Breach Notification Rule, but recently, in September 2021, the agency issued a written statement clarifying the rule, suggesting that the FTC intends to enforce the rule and bring civil actions. Separately, the COVID-19 Consumer Protection Act authorized civil penalties from companies and individuals engaging in deceptive practices associated with "the treatment, cure, prevention, mitigation, or diagnosis of COVID-19." The FTC has already filed multiple cases seeking civil penalties for such violations.

[29] FTC Notices of Penalty Offenses Concerning Endorsements.

[30] FTC Notices of Penalty Offenses Concerning Education.

rules, subject to a three-year statute of limitations (see provision above addressing civil penalties for rule violations). Section 19(b) authorizes a court to grant such relief as the court finds necessary to redress consumer injury, and such relief may include: rescission or reformation of contracts, the refund of money or return of property, the payment of damages, and public notification respecting the rule violation or the unfair or deceptive act or practice, as the case may be. Exemplary or punitive damages, however, are expressly not authorized.

- Redress Actions for Initial Violations Where the FTC Engages in a Lengthy Two-Step Process. Section 19(a)(2) of the FTCA authorizes the FTC to obtain consumer redress in federal court in situations where the FTC: (1) issues a final cease-and-desist order against a company or individual (affirmed after all appeals); and (2) subsequently brings an action in federal court, subject to a three-year statute of limitations, and "satisfies the court that the act or practice to which the cease-and-desist order relates is one which a reasonable man would have known under the circumstances was dishonest or fraudulent." Congress intentionally chose this exacting standard in order to make it challenging for the FTC to obtain monetary remedies from first-time offenders unless the behavior was so egregious that it could be deemed "dishonest or fraudulent."

Finally, we note that the FTC can also enter into settlements that provide for monetary payments not expressly authorized by any statutory provisions. In fact, in one recent case, the two Republican commissioners wrote a dissent arguing that Section 19 does not permit the Commission to accept monetary remedies in an administrative settlement beyond consumer redress for injured consumers and that the settlement amount far exceeded any injury suffered by the consumers in that case.[31] The dissent also forcefully opposed the FTC's willingness to enter into settlements that include monetary payments not authorized by statute: "The majority is correct that, as a practical matter, the government has the ability to extort that to which it is not entitled under law. As we have said on other occasions, though, just because we can does not mean that we should."[32]

---

[31] Dissenting Statement of Commissioners Noah Joshua Phillips and Christine S. Wilson In the Matter of Resident Home LLC (Oct. 7, 2021).

[32] Id.

9. When Confronting Potential FTC Enforcement, Recognize That Deciding Whether to Settle or Litigate Requires a Case-by-Case Assessment of a Wide Range of Factors

The vast majority of FTC consumer protection enforcement actions result in settlements. In fact, in the cybersecurity space, only three companies have litigated against the FTC to date: Wyndham, LabMD, and D-Link.

In deciding whether to settle with the FTC or litigate, companies must balance an assortment of business and reputational considerations. Litigation is costly, time- and resource-intensive, and can play out over many years before resolution. In contrast, a settlement provides the certainty and closure that many companies value.

Companies should recognize, however, that the FTC recently acknowledged that "federal courts may approve settlements that include relief beyond what could have been awarded at trial."[33] The FTC may, for example, demand that monetary relief or "fencing-in" provisions be included in a settlement even though a federal court may be unwilling to award such relief through litigation. In fact, the three companies that litigated cybersecurity cases against the FTC all arguably came out better than if they would have settled in the absence of litigation.

Accordingly, companies must assess a wide range of issues, including the unique facts associated with each case and the company's tolerance for litigation, in order to determine whether it would be advisable to settle with the FTC or litigate.

10. Monitor Congressional Developments

As of this writing, the Build Back Better Act has stalled in the Senate. The bill would have provided $1 billion to the FTC to create and operate a new FTC bureau solely dedicated to privacy and cybersecurity enforcement. The funding would have been provided until 2031. The bill also would have for the first time granted the FTC the authority to obtain civil penalties for initial violations of the FTCA.

The status of the Build Back Better Act is unclear, but in light of the Supreme Court's *AMG Capital* decision, the FTC will without doubt continue to pursue congressional authorization for additional mechanisms to obtain monetary remedies from companies

[33] Joint Statement of Chair Lina Khan, Commissioner Rohit Chopra, and Commissioner Rebecca Kelly Slaughter In the Matter of Resident Home LLC (Oct. 8, 2021).

violating the FTCA. Many organizations, including the Chamber of Commerce, are strongly opposing congressional action:

> Congress specifically balanced its current enforcement regime to prevent unfair enforcement under the FTC Act's vague and broad prohibition on unfair and deceptive practices. The approach proposed in H.R. 5376 [the Build Back Better Act] permanently removes statutory due process protections. At a time when the Commission has demonstrated willingness to exceed its authority, such a policy change would be highly detrimental to legitimate businesses because the FTC would become the lawmaker, prosecutor, judge, and jury all at once, where businesses may never know which of their practices may later be adjudged to be illegal. The threat will be particularly severe for smaller companies that lack the legal expertise and capital to hire outside counsel to contest the FTC's proposed settlements backed by the threat of potentially bankrupting fines regardless of whether they believe their activities are completely lawful.[34]

Finally, Congress is also contemplating whether to enact a comprehensive data privacy law that would likely preempt existing state laws. At his Senate confirmation hearing last month, President Biden's nomination for FTC Commissioner, Alvaro Bedoya, indicated that he supports the development and enactment of "strong comprehensive data privacy legislation that would preempt state law." He noted, however, that if the law was not sufficiently strong, he may be opposed to outright preemption. Bedoya also noted that he believes strong comprehensive data privacy legislation would: (1) not be technology-specific, anticipating future data streams and technologies, particularly with respect to biometrics; (2) include both consent-based collection restrictions and post-collection use restrictions; (3) include general fiduciary duties, such as a duty of loyalty; and (4) include provisions allowing for robust enforcement.

* * *

We will continue to monitor any updates related to the FTC and future enforcement activities. Please do not hesitate to contact us with any questions.

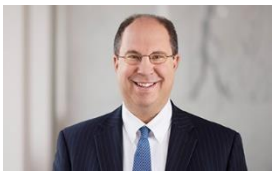
---

[34] Letter from the U.S. Chamber of Commerce to the U.S. Senate (Dec. 15, 2021).

WASHINGTON, D.C.


Luke Dembosky
ldembosky@debevoise.com


Ted Hassi
thassi@debevoise.com


Paul D. Rubin
pdrubin@debevoise.com

NEW YORK


Leah Martin
lmartin@debevoise.com


Melissa Runsten
mrunsten@debevoise.com


Avi Gesser
agesser@debevoise.com

SAN FRANCISCO


Jim Pastore
jjpastore@debevoise.com


Johanna N. Skrzypczyk
jnskrzypczyk@debevoise.com


Christopher S. Ford
csford@debevoise.com