Consumer Protection Enforcement: Taking It Up a Notch

Joe Simons and Andrew Smith

The FTC's consumer protection mission has a long history of vigorous enforcement, protecting consumers from deceptive advertising, fraudulent business activities, and harmful privacy and data security practices. Since returning to the FTC in May 2018, we have worked with the staff of the Bureau of Consumer Protection (BCP) to build on that record and pursue an active and innovative enforcement agenda. Key accomplishments include:

- Considering in every case whether to hold individuals responsible for the violations of the companies they help operate and systematically pushing for individual liability where warranted by the facts.
- Continuing to seek penalties and redress aggressively and creatively, including in cases where the Commission never has before, and obtaining the largest penalties and redress awards in BCP's history.
- Taking a fresh look at the conduct relief in our orders, and, as a result, strengthening orders to better protect consumers.

The FTC's many years of experience in bringing enforcement actions to protect consumers has informed our efforts over the last two years to enforce the law aggressively and innovate on remedies. We have built on past successes obtaining relief from individuals as well as larger civil penalties and redress awards where warranted. Similarly, the Commission's experience enforcing orders and bringing data security and privacy cases played a role in the fashioning of more effective orders over the last two years.

Individual Liability

The FTC has the authority to obtain appropriate relief from individuals as well as the businesses they lead. Under prevailing case law, the FTC may hold an individual liable for injunctive relief if he or she participated directly in—or had the authority to control—the corporate misconduct. An individual liable for injunctive relief is also liable for monetary relief under Section 13(b) of the FTC Act if he or she had actual knowledge of the unlawful conduct, was recklessly indifferent to its unlawfulness, or had an awareness of a high probability of illegality and intentionally avoided learning the truth. Section 13(b) is one of the means by which the FTC provides redress to consumers,[1] although its use for this purpose has been questioned in a recent case that is subject to Supreme Court review.[2]

Joe Simons *is the Chairman of the Federal Trade Commission.* ***Andrew Smith*** *is the Director of the FTC's Bureau of Consumer Protection.* *The authors acknowledge the invaluable assistance of Robert Frisby, Counsel to the Director of the Bureau of Consumer Protection, in preparing this article. This article reflects the personal views of the authors, which do not necessarily reflect the views of the Commission or other Commissioners.*

[1] The FTC also can seek monetary relief in some cases pursuant to Sections 5(l) (administrative order violations) and 19 (e.g., trade regulation rule violations) of the FTC Act, and in civil contempt cases.

[2] AMG Cap. Mgmt., LLC v. FTC, 910 F.3d 417 (9th Cir. 2018), *cert. granted,* No. 19-508 (July 9, 2020).

In every case the FTC brings, there is at least one and often many individuals who meet these standards for liability, but it is neither necessary nor appropriate to seek injunctive relief against every officer with authority to control alleged misconduct. Accordingly, over its more than 100-year history, the agency has exercised discretion in deciding when to seek conduct or monetary relief from individuals. In exercising this discretion over the years, the FTC has commonly sought relief from controlling individuals where individual liability is the only effective way to protect consumers (e.g., the corporation would be easy to dissolve and reconstitute, as a way of evading the order). Many, but by no means all, of these cases involved clearly fraudulent conduct.

More recently, we have approached this issue in a more systematic way to identify cases where we should hold individuals liable for corporate misconduct even though we would not necessarily have done so previously. This has enabled the FTC to send a message that it will hold accountable corporate officers or others in a position of authority who actively participate in, facilitate, or condone misconduct, with knowledge of its wrongfulness.

For example, in October 2019 the FTC provisionally approved a settlement with cosmetics firm Sunday Riley Modern Skincare, LLC and its CEO, Sunday Riley.[3] The FTC charged them with misleading consumers by posting fake reviews of the company's products on a major retailer's website, at the CEO's direction, and by failing to disclose that the reviewers were company employees. Seeking conduct relief from the CEO here demonstrates the FTC's commitment to holding those who knowingly and willfully deceive consumers accountable—even though Sunday Riley Modern Skincare, LLC, is unlikely to be dissolved for the purposes of evading this order, and effective conduct relief could be obtained by naming the company alone. The Commission issued the complaint and the final order on November 6, 2020.[4]

Similarly, in December 2019, the FTC filed suit against FleetCor Technologies, Inc., a publicly traded seller of fuel card services to businesses with reported annual revenue of $2.4 billion, and its CEO Ronald Clarke, for allegedly charging customers at least hundreds of millions of dollars in hidden fees after making false promises about helping customers save on fuel costs.[5] The complaint alleges that the CEO directed and knew about the practices challenged in the complaint.[6] Like *Sunday Riley*, this case sends an unmistakable message that the Commission will hold CEOs responsible when warranted by the facts.

More recently, in August 2020, the FTC filed suit against Yellowstone Capital LLC and Fundry LLC, and their CEO Yitzhak D. Stern and President Jeffrey Reece, providers of "merchant cash advances," short term, high-cost financing products to small business consumers.[7] The FTC alleged that they: (1) unlawfully withdrew millions of dollars in excess payments from their customers' accounts, and to the extent they provided refunds, sometimes took weeks or even months to provide them; (2) deceived potential customers about the amount of money they would receive,

---

[3] Press Release, Fed. Trade Comm'n, Devumi, Owner and CEO Settle FTC Charges They Sold Fake Indicators of Social Media Influence; Cosmetics Firm Sunday Riley, CEO Settle FTC Charges That Employees Posted Fake Online Reviews at CEO's Direction (Oct. 21, 2019), https://www.ftc.gov/news-events/press-releases/2019/10/devumi-owner-ceo-settle-ftc-charges-they-sold-fake-indicators.

[4] Press Release, Fed. Trade Comm'n, FRC Approves Final Consent Agreement with Sunday Riley Modern Skincare, LLC (Nov. 6, 2020), https://www.ftc.gov/news-events/press-releases/2020/11/ftc-approves-final-consent-agreement-sunday-riley-modern-skincare.

[5] Press Release, Fed. Trade Comm'n, FTC Alleges Fuel Card Marketer Fleetcor Charged Hundreds of Millions in Hidden Fees (Dec. 20, 2019), https://www.ftc.gov/news-events/press-releases/2019/12/ftc-alleges-fuel-card-marketer-fleetcor-charged-hundreds-millions.

[6] *See* Complaint ¶¶ 16, 32–35, and 70, Fleetcor Techs., No. 1:19-cv-05727-ELR (N.D. Ga. Dec. 20, 2019).

[7] Press Release, Fed. Trade Comm'n, FTC Alleges Merchant Cash Advance Provider Overcharged Small Businesses Millions (Aug. 3, 2020), https://www.ftc.gov/news-events/press-releases/2020/08/ftc-alleges-merchant-cash-advance-provider-overcharged-small.

with the amount shown on the contract not reflecting additional fees that would be deducted; and (3) misrepresented that business owners would not be required to provide collateral or be subject to a personal guaranty. The complaint also alleges that the CEO and President closely oversaw and directed day-to-day advertising and marketing efforts, reviewed and provided feedback and approval for advertising content and claims, closely oversaw and managed the servicing and collection of payments from consumers, and knew about unauthorized overpayments by consumers.[8] This case, too, illustrates the FTC's commitment to holding corporate officers accountable when they knowingly engage in unlawful practices, as opposed to where they lack knowledge of illegality (e.g., cases involving a failure to discover the flaws in clinical studies purportedly supporting a health claim).

Civil Penalties and Equitable Monetary Relief

In addition to holding individuals accountable, the FTC has aggressively sought both civil penalties to provide effective deterrence and consumer redress to compensate consumers.

In addition to holding individuals accountable, the FTC has aggressively sought both civil penalties to provide effective deterrence and consumer redress to compensate consumers. As explained below, this effort has led to billions of dollars in penalties and consumer redress, including record sums in high profile cases. Moreover, in a number of these cases the FTC worked collaboratively with other federal agencies and state attorneys general as co-plaintiffs to achieve the best results for consumers.

Civil Penalties. The FTC has the authority to obtain civil penalties for violations of its administrative orders pursuant to Section 5(l) of the FTC Act, as well as for violations of certain rules pursuant to Section 5(m). For rule violations, Section 5(m)(1)(C) of the Act provides, "In determining the amount of such a civil penalty, the court shall take into account the degree of culpability, any history of prior such conduct, ability to pay, effect on ability to continue to do business, and such other matters as justice may require." Although Section 5(l) does not specify the factors for courts to consider in determining civil penalties, courts have generally considered the following: (1) the injury to the public resulting from the violation, (2) the defendant's ability to pay penalties, (3) the good or bad faith of the defendant in violating the order, (4) the desire to eliminate benefits derived by the defendant from violative activities, and (5) the necessity of vindicating the FTC's authority by deterring similar behavior by others.[9]

Over the last two years, the FTC has applied these factors aggressively with the goal of maximizing both specific and general deterrence to better protect consumers. Although the FTC does not generally make its analysis of these factors public in the context of settlements (more on that below), our approach has resulted in some of the largest penalties obtained in BCP cases. For example, during the last two years, the FTC has obtained the highest ever penalties for alleged order violations under Section 5(l) and violations of the Children's Online Privacy Protection Act (COPPA) rule.

Last year the FTC announced a groundbreaking privacy settlement with Facebook, which imposes a record-breaking $5 billion penalty to resolve allegations that the firm violated a 2012 FTC order.[10] Specifically, the FTC alleged that Facebook: (1) told consumers that they could limit the sharing of their information to groups such as their "friends" but, in fact, Facebook shared the

---

[8] See Complaint ¶¶ 20 and 36, Yellowstone Capital LLC, No. 1:20-cv-06023 (S.D.N.Y. Aug. 3, 2020).

[9] *See e.g.,* United States v. Reader's Digest Ass'n, 494 F. Supp. 770, 772 (D. Del. 1980) (violating a consent order), *aff'd*, 662 F.2d 955, 967 (3d Cir. 1981).

[10] Lesley Fair, *FTC's $5 Billion Facebook Settlement: Record-Breaking and History-Making,* FTC Business Blog (July 24, 2019), https://www.ftc.gov/news-events/blogs/business-blog/2019/07/ftcs-5-billion-facebook-settlement-record-breaking-history.

information more broadly with third-party app developers; (2) failed to adequately assess and address privacy risks posed by third-party app developers; and (3) misrepresented to certain users that they would have to "turn on" facial recognition technology, but for millions of users, that technology was "on" by default.[11] In addition to imposing this massive penalty, the Facebook settlement strengthened the FTC order in important and creative ways, as discussed below. The settlement shows how seriously the Commission views violations of its orders as well as unlawful practices relating to consumer privacy.

The FTC's aggressive approach to seeking penalties also resulted in a record-setting penalty in a case enforcing the COPPA rule. In September 2019, Google LLC and its subsidiary YouTube, LLC agreed to pay a $136 million penalty (and an additional $34 million to the State of New York) to settle allegations that the YouTube video sharing service illegally collected personal information in the form of persistent identifiers used to track users across the Internet from viewers of child-directed channels, without first notifying parents and getting their consent.[12] The $136 million penalty is by far the largest amount the FTC has ever obtained in a COPPA case since Congress enacted the law in 1998. The settlement also includes innovative conduct relief designed to promote COPPA compliance, discussed below.

Regardless of the type of unlawful practice subject to civil penalty liability, absent one of the mitigating factors described below, we believe that the goal of the penalty should be to deter law violations by making compliance more profitable or otherwise more attractive than violation. The penalty imposed in *HyperBeard,* a 2020 case involving alleged COPPA violations, illustrates this approach to penalty calculation.[13] HyperBeard allegedly allowed third-party ad networks to collect personal information in the form of persistent identifiers to track users of the company's child-directed apps, without notifying parents or obtaining verifiable parental consent. The ad networks used the identifiers to target ads to children using HyperBeard's apps.

In *HyperBeard*, we laid out a methodology for considering civil penalties.[14] We examine consumer injury as well as excess profits resulting from a law violation and then adjust those amounts to account for the likelihood of detection. In *HyperBeard*, we had no evidence of pecuniary injury to consumers, so we estimated the revenue from behavioral advertising that was illegal under COPPA, as compared to the revenue that would have been earned from contextual advertising, which is otherwise legal. Thus, the starting point for the civil penalty was the excess profits from behavioral advertising over the relevant time period adjusted upwards by a factor to account for the likelihood of detection. If, as is typically the case, the probability of detection is less than 100 percent, the penalty must exceed the gain from the violation to deter violations effectively. The goal is to make compliance more attractive than violation. The probability of detection is often difficult

---

[11] Press Release, Fed. Trade Comm'n, FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook (July 24, 2019) [hereinafter Facebook Press Release], https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions.

[12] Press Release, Fed. Trade Comm'n, Google and YouTube Will Pay Record $170 Million for Alleged Violations of Children's Privacy Law (Sept. 4, 2019), https://www.ftc.gov/news-events/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations.

[13] Press Release, Fed. Trade Comm'n, Developer of Apps Popular with Children Agrees To Settle FTC Allegations It Illegally Collected Kids' Data Without Parental Consent (June 4, 2020), https://www.ftc.gov/news-events/press-releases/2020/06/developer-apps-popular-children-agrees-settle-ftc-allegations-it. We note that not all Commissioners agreed with the Commission's approach here. *See* Dissenting Statement of Commissioner Noah Joshua Phillips (June 4, 2020), https://www.ftc.gov/system/files/documents/public_statements/1576434/192_3109_hyperbeard_-_dissenting_statement_of_commissioner_noah_j_phillips.pdf.

[14] Statement of Chairman Joseph J. Simons in FTC v. HyperBeard Inc., No. 1923109 (June 4, 2020), https://www.ftc.gov/system/files/documents/public_statements/1576438/192_3109_hyperbeard_-_statement_of_chairman_simons.pdf.

to measure, and will vary depending on the circumstances and type of conduct at issue (e.g., detection may be more likely where a firm is subject to an order and must file compliance reports with the FTC; and the probability for self-reported violations that law enforcers have not already discovered should be 100 percent).

In a case where the dollar value of consumer injury exceeded the dollar value of excess profits, consumer injury would be the starting point, adjusted for likelihood of detection.

These are only the starting points for calculating penalties. We must also consider a number of additional factors, including the degree of culpability, history of prior related conduct, prior law enforcement actions, timeliness of corrective action, ability to pay, willfulness, the threat posed to consumers, the effect on the ability to continue to do business, and "such other matters as justice may require," (e.g., cooperation with our investigation, past approaches to similar violations, and the expectations of businesses and consumers). These factors may warrant an increase or decrease in the penalty amount. However, they will rarely if ever warrant a penalty lower than the consumer injury or profit stemming from the unlawful conduct.

[O]ver the last two years the FTC has succeeded in obtaining well over a billion dollars in redress for consumers who suffered financial injury due to unlawful practices.

We also should consider the deterrent effects of the other sanctions imposed when the FTC issues or obtains an order. These effects include the costs and constraints of complying with the conduct relief; the fencing in of otherwise legal conduct; the reputational effect of the sanction; the threat of follow-on actions by shareholders, private plaintiffs, and other regulators; and other collateral consequences, such as the effect on relationships with business partners, vendors, investors, and regulators. All of these non-monetary sanctions can have substantial deterrence effect.

Finally, we must always weigh carefully the extent of consumer harm resulting from the violations. Where common sense and the available evidence suggests that the particular practices in question are most likely to harm consumers, we should adjust the penalty upward in order to more strongly penalize and deter those most harmful practices. A penalty based solely or primarily on the gain to the violator and the likelihood of detection may not suffice where the gain is small and the injury is great.

Equitable Monetary Relief. In addition to obtaining higher and even record penalties where warranted, the FTC has continued to seek redress for consumers injured by deceptive and unfair practices. Indeed, over the last two years the FTC has succeeded in obtaining well over a billion dollars in redress for consumers who suffered financial injury due to unlawful practices. In addition, the FTC has more aggressively obtained and will continue to seek monetary relief in cases where many consumers would likely have purchased the product or service even absent the alleged deception or other unlawful activity.

For example, in July 2019, the FTC announced a settlement with the major credit reporting agency Equifax Inc., which agreed to pay at least $575 million, and potentially up to $700 million, as part of a global settlement with the FTC, the Consumer Financial Protection Bureau (CFPB), and 50 U.S. states and territories.[15] The settlement resolved allegations that Equifax failed to take reasonable steps to secure its network which led to a data breach in 2017 that affected approximately 147 million people.

In December 2019, the FTC announced a settlement with the University of Phoenix and its parent company, Apollo Education Group, which agreed to settle for $191 million in redress and debt forgiveness to resolve allegations that they falsely touted their relationships and job opportunities

[15] Press Release, Fed. Trade Comm'n, Equifax To Pay $575 Million as Part of Settlement with FTC, CFPB, and States Related to 2017 Data Breach (July 22, 2019), https://www.ftc.gov/news-events/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related.

with companies such as AT&T, Yahoo!, Microsoft, Twitter, and The American Red Cross, including in ads targeting military and Hispanic consumers.[16] The settlement requires them to pay $50 million in cash and cancel $141 million in debts owed to the school by students harmed by the deceptive ads. This is the largest settlement the FTC has obtained in a case against a for-profit school.

In April 2020, the FTC announced a settlement with Progressive Leasing, a company that markets rent-to-own payment plans in tens of thousands of retail stores nationwide, which agreed to pay $175 million to resolve allegations that it misled consumers about the true price of items purchased through its plans.[17] Specifically, the FTC alleged that consumers who visited retailers to buy items such as furniture, jewelry, or cellphones frequently were told that Progressive's payment plans were "same as cash" or "no interest"—leading consumers to believe they would not be charged more than an item's sticker price. Instead, the FTC alleges, consumers paid more than the sticker price, and frequently paid approximately twice the sticker price if they made all scheduled payments under the plans.

We also announced a settlement with multi-level marketer AdvoCare International, L.P. which agreed to pay $150 million to resolve allegations that it operated an illegal pyramid scheme that deceived consumers into believing they could earn significant income as "distributors" of its health and wellness products.[18]

Absent highly unusual circumstances, law violators should expect the FTC to seek redress in any case where it has a viable legal theory for doing so.

These cases have addressed a wide variety of allegedly unlawful practices relating to data security and the marketing of educational services, rent-to-own contracts, and business opportunities. These four settlements in particular demonstrate the FTC's commitment to redressing consumers where warranted regardless of the industry or size of the firm that allegedly violated the law. Absent highly unusual circumstances, law violators should expect the FTC to seek redress in any case where it has a viable legal theory for doing so.

In every case where the FTC obtains redress, the remedy should approximate the amount of harm resulting from the alleged law violation. If no consumer would have purchased the product or service but for the deception or other law violation, the harm equals the total revenue. Sometimes, however, the product or service has value, and many consumers would have purchased it even absent the deception at the price offered or perhaps at a lower price. In these cases, the harm to such consumers includes the price premium paid due to the deception for all consumers, as well as additional injury to consumers that would not have purchased, but for the deception. Calculating harm in such cases poses a number of challenges, and the FTC will consider reasonable proxies to help estimate the harm as appropriate (e.g., the cost of the deceptive component of an advertising campaign; incremental revenue or additional market share gained from the deceptive or other unlawful practice; the premium consumers paid over comparable products or services).

Going forward, the FTC also plans to take a fresh look at cases where the harm is less than 100 percent of the revenue and has been traditionally viewed as more difficult to quantify and to seek redress aggressively where it may have declined to do so earlier. Indeed, the FTC has

---

[16] Press Release, Fed. Trade Comm'n, FTC Obtains Record $191 Million Settlement from University of Phoenix To Resolve FRC Charges It Used Deceptive Advertising To Attract Prospective Students (Dec. 10, 2019), https://www.ftc.gov/news-events/press-releases/2019/12/ftc-obtains-record-191-million-settlement-university-phoenix.

[17] Press Release, Fed. Trade Comm'n, Rent-To-Own Payment Plan Company Progressive Leasing Will Pay $175 Million To Settle FTC Charges It Deceived Consumers About Pricing (Apr. 20, 2020), https://www.ftc.gov/news-events/press-releases/2020/04/rent-own-payment-plan-company-progressive-leasing-will-pay-175.

[18] Press Release, Fed. Trade Comm'n, Mulit-Level Marketer Advocare Will Pay $150 Million To Settle FTC Charges It Operated an Illegal Pyramid Scheme (Oct. 2, 2019), https://www.ftc.gov/news-events/press-releases/2019/10/multi-level-marketer-advocare-will-pay-150-million-settle-ftc.

already started seeking substantial monetary relief in such cases. For example, in a settlement announced in March 2020 resolving allegations that Williams-Sonoma Inc. misrepresented that its home products and kitchen wares were made in the United States, the company agreed to pay $1 million in monetary relief.[19] Here, there was no allegation that the products failed to perform as advertised. Instead, the company described products that it imported, or that contained significant imported materials, as made in the United States. While many consumers likely would have purchased the products anyway at the same or a lower price, the FTC alleged that the Made in USA representations were deceptive (and hence material to at least some consumers). Like the four cases described above, this one demonstrates the FTC's ongoing commitment to obtain consumer redress where consumers experience harm from deception or other unlawful practices.

Order Improvement

Just as the FTC has taken a fresh approach to the issues discussed above, we have also taken steps to improve and strengthen the conduct relief we obtain in our law enforcement actions. We have obtained innovative relief in a number of program areas, including data security, COPPA and privacy, money transfers, Voice over Internet Protocol (VoIP) services, and third-party oversight.

Data Security. For example, we have revamped our administrative orders in data security enforcement actions to include more company-specific requirements, increase third-party assessor accountability, and focus high-level executive attention on important data security considerations.[20] In *Lightyear Dealer Technologies LLC, d/b/a DealerBuilt*, a company that develops and sells dealer management system software and data processing services to automotive dealerships nationwide allegedly failed to secure consumer data adequately.[21] The consent order requires a comprehensive information security program designed to protect personal information, including third-party assessments of its information security program every two years. Under the order, the assessor must specify the evidence that supports its conclusions and conduct independent sampling, employee interviews, and document review. In addition, the order requires a senior corporate manager responsible for overseeing DealerBuilt's information security program to certify compliance with the order every year.

Subsequent data security orders have followed this same model, and include more company-specific requirements, such as yearly employee training, improved access controls, monitoring systems for data security incidents, patch management systems, and encryption. The specificity both makes the FTC's expectations clearer to companies and improves order enforceability.

Today's data security orders also increase the accountability of third-party assessors. No longer can assessors take the company's word for it—they must do the hard work of examining for order compliance, and must show us their work, such as by identifying evidence to support their conclusions, including independent sampling, employee interviews, and document review. Assessors also must retain and provide the FTC with access to work papers. And, to make clear that

---

[19] Press Release, Fed. Trade Comm'n, Williams-Sonoma, Inc. Settles with FTC, Agrees To Stop Making Overly Broad and Misleading 'Made In USA' Claims About Houseware and Furniture Products (Mar. 30, 2020), https://www.ftc.gov/news-events/press-releases/2020/03/williams-sonoma-inc-settles-ftc-agrees-stop-making-overly-broad.

[20] Andrew Smith, *New and Improved FTC Data Security Orders: Better Guidance for Companies, Better Protection for Consumers*, FTC Business Blog (Jan. 6, 2020), https://www.ftc.gov/news-events/blogs/business-blog/2020/01/new-improved-ftc-data-security-orders-better-guidance. The FTC revamped these orders in part due to the 11th Circuit's ruling in LabMD, Inc. v. FTC, 891 F.3d 1286 (11th Cir. 2018).

[21] Press Release, Fed. Trade Comm'n, Auto Dealer Software Provider Settles FTC Data Security Allegations (June 12, 2020), https://www.ftc.gov/news-events/press-releases/2019/06/auto-dealer-software-provider-settles-ftc-data-security.

we are serious, our new orders explicitly allow the FTC staff to withhold approval of the third-party assessor.

Recent data security orders elevate data security considerations to the C-Suite and Board level by requiring the company to present its written information security program to the Board or similar governing body, and senior officers must provide annual certifications of compliance to the FTC.

All of these changes should focus senior management's attention on important consumer protection issues and improve order enforceability.

COPPA and Privacy. In our COPPA enforcement program, we have obtained creative remedies against technology platforms and app developers that ignored the presence of children among their users or that illegally targeted child users with online advertising. For example, the *Google/YouTube* order requires them to implement and maintain a system that permits channel owners to identify their child-directed content on the YouTube platform so that YouTube can ensure its compliance with COPPA. In addition, they must notify channel owners that their child-directed content may be subject to the COPPA Rule's obligations and provide annual training about complying with COPPA for employees who deal with YouTube channel owners.

Facebook. In the settlement resolving Facebook's alleged order violations, the FTC obtained ground-breaking conduct relief that includes a host of new provisions designed to ensure compliance and protect consumer privacy.[22] The order creates greater accountability at the board of directors level by establishing an independent privacy committee of Facebook's board and removing unfettered control by Facebook's CEO Mark Zuckerberg over decisions affecting user privacy. Members of the privacy committee must be independent and will be appointed by an independent nominating committee. Members can only be fired by a supermajority of the Facebook board of directors.

The order also improves accountability at the individual level. Facebook must designate compliance officers who will be responsible for Facebook's privacy program. These compliance officers will be subject to the approval of the new board privacy committee and can be removed only by that committee—not by Facebook's CEO or Facebook employees. Facebook CEO Mark Zuckerberg and designated compliance officers must independently submit to the FTC quarterly certifications that the company is in compliance with the privacy program mandated by the order, as well as an annual certification that the company is in overall compliance with the order. Any false certification will subject them to individual civil and criminal penalties.

Furthermore, as part of Facebook's order-mandated privacy program, which covers WhatsApp and Instagram, Facebook must conduct a privacy review of every new or modified product, service, or practice before it is implemented, and document its decisions about user privacy. The designated compliance officers must generate a quarterly privacy review report, which they must share with the CEO and the independent assessor, as well as with the FTC upon request by the agency. The order also requires Facebook to document incidents when data of 500 or more users has been compromised, and its efforts to address such an incident, and deliver this documentation to the Commission and the assessor within 30 days of the company's discovery of the incident.

Additionally, the order imposes significant new privacy requirements, including the following:

(1) Facebook must exercise greater oversight over third-party apps, including by terminating app developers that fail to certify that they are in compliance with Facebook's platform policies or fail to justify their need for specific user data;

---

[22] Facebook Press Release, *supra* note 11.

(2) Facebook is prohibited from using telephone numbers obtained to enable a security feature (e.g., two-factor authentication) for advertising;
(3) Facebook must provide clear and conspicuous notice of its use of facial recognition technology, and obtain affirmative express user consent prior to any use that materially exceeds its prior disclosures to users;
(4) Facebook must establish, implement, and maintain a comprehensive data security program;
(5) Facebook must encrypt user passwords and regularly scan to detect whether any passwords are stored in plaintext; and
(6) Facebook is prohibited from asking for email passwords to other services when consumers sign up for its services.

Money Transfers, VoIP providers, and Third-Party Oversight. We have renewed our commitment to pursuing companies that actively facilitate fraudulent schemes perpetrated by others, such as providers of money transfer or VoIP services. The orders in these cases impose detailed diligence and monitoring requirements with respect to third-party business customers.

For example, the FTC's settlement with MoneyGram announced in November 2018 includes an expanded and modified order superseding the 2009 order and applying to money transfers worldwide.[23] The modified order requires, among other things, that the company block the money transfers of known fraudsters and provide refunds to fraud victims in circumstances where its agents fail to comply with applicable policies and procedures. In addition, the modified order includes enhanced due diligence, investigative, and disciplinary requirements.

Similarly, the FTC's settlement with VoIP provider Globex Telecom, Inc., which resolved charges that it facilitated a scheme involving bogus credit card interest rate relief and millions of illegal charges to consumers, imposes extensive monitoring and related obligations.[24] This settlement is also the first consumer protection order entered against a VoIP service provider.

Specifically, the order requires the VoIP provider to abide by detailed client screening and monitoring provisions, such as (1) a prohibition on providing VoIP and related services to clients who pay with stored value cards or cryptocurrency, or to clients who do not have a public-facing website or social media presence; (2) a screening and a review process for all potential clients, including re-screening any existing client who is subject to a subpoena from the government or similar investigative request; (3) a requirement to block any calls made by their clients that appear to come from certain suspicious phone numbers, including emergency numbers like 911, unassigned or invalid numbers, or international numbers that would charge consumers a large amount should they attempt to dial it; and (4) a requirement to block calls using spoofing technology, and to terminate any relationship with any telemarketer or other high-risk client that receives three or more USTelcom Traceback Requests (an official industry complaint about unlawful calls) or line carrier complaints in a 60-day period. This innovative VoIP order sends an unmistakable signal to the VoIP industry that the FTC will seek tough conduct relief in cases where they facilitate illegal marketing practices.

These examples illustrate the FTC's commitment to securing effective conduct relief to protect consumers, and to provide guidance to the public regarding best practices to avoid deception and unfairness. ●

---

[23] Press Release, Fed. Trade Comm'n, Moneygram Agrees To Pay $125 Million To Settle Allegations that the Company Violated the FTC's 2009 Order and Breached a 2012 DOJ Deferred Prosecution Agreement (Nov. 8, 2018), https://www.ftc.gov/news-events/press-releases/2018/11/moneygram-agrees-pay-125-million-settle-allegations-company.

[24] Press Release, Fed. Trade Comm'n, Globex Telecom and Associates Will Pay $2.1 Million Settling FTC's First Consumer Protection Case Against a VoIP Service Provider (Sept. 22, 2020), https://www.ftc.gov/news-events/press-releases/2020/09/globex-telecom-associates-will-pay-21-million-settling-ftcs-first.