WILKINSON BARKER KNAUER LLP

ENFORCEMENT UPDATE

This update includes notable FCC and FTC enforcement actions during the third quarter of 2024 that may be of interest to telecom, media, and tech companies.

Questions or comments may be addressed to Suzanne Tetreault at 202-383-3375 or STetreault@wbklaw.com, Jeffrey Gee at 202-383-3409 or JGee@wbklaw.com, or Jennifer Tatel at 202-383-3344 or JTatel@wbklaw.com.

FCC MATTERS

GENERAL UPDATES

At the end of June, the Supreme Court ruled in SEC v. Jarkesy that the SEC's civil penalty enforcement process violated the Seventh Amendment right to a jury trial. The case has spurred fresh debate over the scope of agency authority more generally—including at the FCC—to impose civil penalties from enforcement investigations without making a jury trial available. In early September, FCC Commissioner Simington called for the FCC to open a Notice of Inquiry to reconsider its enforcement authority and committed to dissenting from every Commission decision imposing a monetary forfeiture until it does so.

The FCC has addressed some of these criticisms, arguing that the FCC's enforcement process is different from the SEC's process because parties subject to FCC forfeiture orders are entitled to a "trial de novo" in federal district court before they can be required to pay. In addition, the FCC has taken the position that most FCC enforcement actions address "public rights," which the Supreme Court acknowledged may not be subject to the jury trial requirements of the Seventh Amendment.

The issue of Jarkesy's impact on FCC enforcement has already been raised in the courts. For instance, the parties to the FCC's April forfeitures involving customer location data cases have raised the issue on appeals.

PRIVACY, DATA, AND CYBERSECURITY

The FCC and its Enforcement Bureau ("EB") have continued to aggressively pursue privacy and data security enforcement actions, leading to several multi-million dollar fines and compliance plans with novel cybersecurity terms in Q3. In addition, at the end of August, Chairwoman Rosenworcel signed a Memorandum of Understanding with the Privacy Commissioner of Canada to enhance the ability of both agencies to pursue cross-border enforcement actions related to consumer privacy, data, and cybersecurity.

In early July, EB entered a settlement totaling $35 million with a Telecommunications Relay Service ("TRS") provider to resolve an investigation into allegedly unlawful retention of call content and submission of inaccurate information to the Telecommunication Relay Service ("TRS") Fund Administrator. The settlement involved a $5 civil penalty, $12 million in reimbursement to the TRS Fund, relinquishment of $13.6 million in IP Captioned Telephone Service reimbursement claims, and a $4 million investment in privacy and data security protection enhancements. The company also agreed to a comprehensive compliance plan involving consumer privacy and data protection terms such as conducting a data inventory, implementing a data retention schedule, and investing in privacy-enhancing technologies.

Also in July, EB settled with a wireless provider for $16 million to resolve an investigation into three cybersecurity breaches involving the exploitation of application programming interfaces that resulted in unauthorized access to customers' proprietary information, including CPNI and personally identifiable information. In addition to the civil penalty, the settlement requires a cybersecurity compliance plan with "novel" provisions; subscriber identity module change and port-out protections; annual internal and independent assessments; and privacy and security training for employees and certain third parties.

In mid-September, EB entered a $13 million settlement with a wireless provider to resolve an investigation into the company's supply chain integrity and a vendor's cloud security measures. The compliance plan included in the settlement requires implementation of a data inventory program and an Information Security Program, implementation of vendor controls and oversight, and requires vendors to adhere to retention and disposal obligations and conduct annual compliance audits.

At the end of September, EB settled with a wireless provider to resolve multiple investigations into cybersecurity incidents. The settlement involved a $15.75 million civil penalty and required the company to make a $15.75 million investment in cybersecurity and implement a comprehensive cybersecurity plan that involves regular cybersecurity reporting from the Chief Information Security Officer to the board of directors, and implementation of "zero-trust" architecture and multi-factor authentication.

CHILDREN'S PROGRAMMING

In early September, the FCC released a Forfeiture Order imposing forfeitures totaling over $3.3 million against several television broadcasters for violations of the FCC's rules limiting commercial matter in children's programming. The Forfeiture Order found that 21 separate television licensees had aired "program length commercials" by virtue of having aired advertisements for the "Hot Wheels Super Ultimate Garage" toy during episodes of the "Team Hot Wheels" program. This was the first FCC forfeiture order to directly address the Supreme Court's decision in Jarkesy. Commissioner Carr dissented on the grounds that the forfeitures were too high and emphasized that the FCC should "start the process of fundamentally reforming our enforcement practices—lest the courts step in" following Jarkesy. Commissioner Simington authored his first dissent on the Jarkesy grounds discussed above.

SATELLITE

In mid-August, EB entered a consent decree with a satellite operator to resolve an investigation into the company's operation a satellite from an unauthorized orbital location. The company had obtained special temporary authority to conduct telemetry, tracking, and command transmissions while the satellite drifted to its authorized orbital location. However, the company instead drifted the satellite to a different, unauthorized orbital location in March 2023 and incorrectly informed the FCC that it had successfully drifted the satellite to the authorized orbital location. The company disclosed the error in mid-April 2023. The consent decree requires Intelsat to pay a civil penalty of $160,000 and to create a compliance plan.

ROBOCALLS/SPOOFING

In early July, as a continuation of its "Spring Cleaning" series of robocall enforcement actions, EB issued an Initial Determination Order against Veriwave Telco for allegedly originating approximately 15.8 million robocalls pertaining to a "National Tax Relief Program." Veriwave was given 15 days to respond before EB would issue a Final Determination Order directing immediately downstream providers to block of all traffic from Veriwave. As of the date of this update, EB has not issued a Final Determination Order against Veriwave.

During the third quarter of 2024, the FCC completed its enforcement actions relating to January's robocall incident involving AI-generated robocalls cloning President Biden's voice to spread misinformation to voters prior to New Hampshire's primary election. On September 30, the FCC issued a $6 million Forfeiture Order against Steve Kramer, the originator of the calls. In August, EB settled for $1 million with the provider, Lingo Telecom, that allegedly enabled Mr. Kramer's calls by labeling them with the highest level of call attestation without making any effort to verify the accuracy of the calls. The consent decree required Lingo to implement a "first-of-its-kind" compliance plan that requires Lingo to strictly adhere to STIR-SHAKEN caller ID rules, abide by "know your customer" and "know your upstream provider" principles, and more thoroughly verify the accuracy of information provided by its customers and upstream providers.

PIRATE RADIO

In August, the FCC affirmed a $2.3 million fine against the operator of a "pirate" radio station in the Bronx for violating its rules under the requirements of the Preventing Illegal Radio Abuse Through Enforcement Act ("PIRATE Act"). In July, EB warned 13 New York and New Jersey landowners of potentially illegal pirate radio transmissions occurring from their properties. In September, the FCC proposed a combined $1,000,000 in fines against four pirate radio stations in New York and New Jersey. The actions resulted from the 2024 NYC-area "pirate radio sweep" mandated by the PIRATE Act. At the same time, the FCC affirmed fines totaling over $800,000 against three pirate radio station operators in Miami. Commissioner Simington dissented from the September decisions on Jarkesy grounds.

NETWORK OUTAGES

At the end of July, EB resolved a network outage case with a $15 million settlement that includes a compliance plan entailing a "first-of-its-kind" cybersecurity component.

At the end of August, EB reached a $950,000 settlement regarding an hour-long 911 outage in four states resulting from a network testing error.

ACCESSIBILITY

In early July, EB released an order finding that Assurance Wireless had failed to ensure that its services were accessible to persons with disabilities. EB agreed with a customer complaint alleging that the company failed to take action to provide the customer with a device that included tactile buttons and a screen reader. The order followed a complaint resolution process that is unique to accessibility complaints and proposed several specific actions that the company would be required take to ensure compliance with accessibility rules. The Order provided the company with an opportunity to comment on those proposed actions. A follow-up Order will make final determinations of the required compliance actions.

FEDERAL FUNDS AND AUCTIONS

In late August, EB issued citations against eleven broadband providers for failing to submit broadband service availability data in the FCC's Broadband Data Collection ("BDC") system. The FCC's rules require all facilities-based fixed or mobile broadband providers to submit this data to the BDC system twice annually, on or before March 1 and on or before September 1. The providers were ordered to submit the missing data by late September or risk forfeiture.

The FCC continued enforcement actions to rigorously police participation in the Affordable Connectivity Program ("ACP") even after its wind down at the end of May. In July, EB formally removed ACP participant K20 Wireless (and Krandon Wenger) from the ACP following its NAL against K20 in May and barred the company from participating in any future program. Additionally, in September, the FCC proposed fines totaling $470,000 against four broadband internet access service providers for apparently willfully violating the FCC's rules by failing to submit certified complete ACP Transparency Data Collection plan and subscribership data.

In mid-July, EB denied a petition for reconsideration filed by Nextlink of a $100,000 forfeiture imposed earlier this year as a penalty for engaging in a series of prohibited communications regarding bids, bidding strategies, and bidding results during the "quiet period" for the Connect America Fund Phase II auction and for failing to report those communications. Specifically, EB rejected arguments that the forfeiture was imposed outside the statute of limitations.

OTHER AGENCIES

In September, the FTC followed up on its ongoing privacy-related proceeding against Facebook (Meta), ordering Meta to appear before the FTC for oral arguments to address the legal issues raised in the proceeding. In this proceeding, the FTC proposed changes to the agency's 2020 privacy order with Facebook, alleging that the company failed to fully comply with the 2000 order, misled parents about the operations of its Messenger Kids app, and misrepresented the access it provided some app developers to private user data. Oral arguments are set for November 12.

In August, the Committee on Foreign Investment in the United States ("CFIUS") revealed that it had imposed a $60 million fine on a wireless provider to resolve an investigation into the company's breach of a National Security Agreement entered with CFIUS in 2018 in connection with a merger and the resulting foreign ownership. CFIUS found that the company failed to take appropriate measures to prevent unauthorized access to certain sensitive data and failed to promptly report some incidents of unauthorized access to CFIUS, delaying CFIUS's efforts to investigate and mitigate any potential harm. CFIUS concluded that these violations resulted in harm to national security.