FEDERAL TRADE COMMISSION
Washington, DC 20580

| |
|---|
| In the Matter of Grindr, LLC |

**Complaint and Request for Investigation, Injunction, Penalties, and Other Relief**

**Submitted by**

**The Electronic Privacy Information Center (EPIC)**

## I. Summary

1. This complaint concerns Grindr's apparent failure to safeguard users' sensitive personal data, including the data of users who have deleted their accounts. Grindr is an LGBTQ+ dating app catering to millions of users worldwide. Its users entrust the company with intimate personal information, including users' sexual and romantic preferences, conversations and photos sent and received via Grindr's app, location data, and health information such as HIV status and vaccination status. In June 2023, Grindr's former Chief Privacy Officer filed a wrongful termination lawsuit against Grindr, alleging that the company fired him when he made executives aware of violations of Grindr's privacy policies. Grindr appears to have engaged in unfair and deceptive trade practices in violation of Section 5 of the FTC Act. The company also appears to have violated the Health Breach Notification Rule (HBNR). For the reasons set out below, the Commission should open an investigation, secure an injunction against the offending business practices, issue fines pursuant to the HBNR, and provide such other relief as the Commission sees fit.

## II. Parties

2. The Electronic Privacy Information Center ("EPIC") is a public interest research center in Washington, DC. EPIC was established in 1994 to focus public attention on emerging civil liberties issues and to secure the fundamental right to privacy in the digital age for all people through advocacy, research, and litigation. EPIC has played a leading role in developing the authority of regulators to safeguard the rights of consumers, ensure the protection of personal data, and address privacy violations.[1] Additionally, EPIC called

[1] *See, e.g.*, Comments of EPIC, *In re Chegg, Inc.* (Dec. 12, 2022), https://epic.org/documents/comments-of-epic-in-re-the-federal-trade-commissions-proposed-order-settlement-with-chegg-inc/; Comments of EPIC, *In re Support*

attention to Grindr's failure to protect users from harassment and abuse by filing an amicus brief in *Herrick v. Grindr*.[2]

3. Grindr LLC is a Delaware corporation headquartered in California. Grindr operates an LGBTQ+ dating app. Grindr has 13 million monthly active users, [3] and it describes itself as "the world's largest social networking app for gay, bi, trans, and queer people."[4]

4. The FTC is an independent agency of the United States government given statutory authority and responsibility by, inter alia, the FTC Act, 15 U.S.C. §§ 41-58. The Commission is charged, inter alia, with enforcing section 5(a) of the FTC Act, 15 U.S.C. § 45(a), which prohibits unfair and deceptive acts or practices in or affecting commerce. Additionally, the FTC promulgated the Health Breach Notification Rule (HBNR), which requires covered entities to notify users when the security of their personal health records (PHR) has been breached.

## III. Factual Background

### A. Grindr Promises its Users that Their Sensitive Data Will Be Protected

5. Grindr promotes itself as a privacy-protective company through its marketing and policies. The company's logo, a mask, reflects Grindr's promise of secrecy and

*King, LLC (SpyFone.com)* (Oct. 8, 2021), https://epic.org/documents/in-the-matter-of-support-king-llc-spyfone-com/; Comments of EPIC et al., *In re Zoom Video Communications, Inc.* (Dec. 14, 2020), https://epic.org/apa/comments/EPIC-FTC-Zoom-Dec2020.pdf; Complaint of EPIC, *In re Online Test Proctoring Companies* (Dec. 9, 2020), https://epic.org/privacy/dccppa/online-test-proctoring/EPIC-complaint-in-re-online-test-proctoring-companies-12-09-20.pdf; Complaint of EPIC, *In re Airbnb* (Feb. 26, 2020), https://epic.org/privacy/ftc/airbnb/EPIC_FTC_Airbnb_Complaint_Feb2020.pdf; Petition of EPIC, *In re Petition for Rulemaking Concerning Use of Artificial Intelligence in Commerce* (Feb. 3, 2020), https://epic.org/privacy/ftc/ai/epic-ai-rulemaking-petition/; Complaint of EPIC, *In re HireVue* (Nov. 6, 2019), https://epic.org/privacy/ftc/hirevue/EPIC_FTC_HireVue_Complaint.pdf; Comments of EPIC, *In re Unrollme, Inc.* (Sept. 19, 2019), https://epic.org/apa/comments/EPIC-FTC-Unrollme-Sept2019.pdf; Comments of EPIC, *In re Aleksandr Kogan and Alexander Nix* (Sept. 3, 2019), https://epic.org/apa/comments/EPIC-FTCCambridgeAnalytica-Sept2019.pdf; Complaint of EPIC, *In re Zoom Video Commc'ns, Inc.* (July 11, 2019), https://epic.org/privacy/ftc/zoomEPIC-FTC-Complaint-In-re-Zoom-7-19.pdf; Comments of EPIC, *In re Uber Technologies, Inc.* (May 14, 2018), https://epic.org/apa/comments/EPIC-FTC-RevisedUber-Settlement.pdf; Comments of EPIC, *In re PayPal, Inc.* (Mar. 29, 2018), https://epic.org/apa/comments/EPIC-FTC-PayPal-ConsentOrder.pdf; Complaint of EPIC, *In re Google Inc.* (July 31, 2017), https://www.epic.org/privacy/ftc/google/EPIC-FTCGoogle-Purchase-Tracking-Complaint.pdf; Complaint of EPIC, *In re Genesis Toys and Nuance Communications* (Dec. 6, 2016), https://epic.org/privacy/kids/EPIC-IPR-FTCGenesis-Complaint.pdf.

[2] Brief for EPIC as Amicus Curiae Supporting Appellant, *Herrick v. Grindr, LLC*, 765 Fed. App'x 586 (2nd Cir. 2019) (No. 18-396), 2018 WL 2759735.

[3] *Investor Relations*, Grindr, https://investors.grindr.com/overview/ (Sept. 26, 2023).

[4] *About*, Grindr, https://www.grindr.com/about (last visited Sept. 13, 2023).

anonymity to users. Users are not required to display their age, name, or photo in their profile.[5]

6. Grindr's promise to protect user privacy is vital because its LGBTQ+ users may not be out: one survey found that 18 percent of Grindr users are still in the closet.[6]

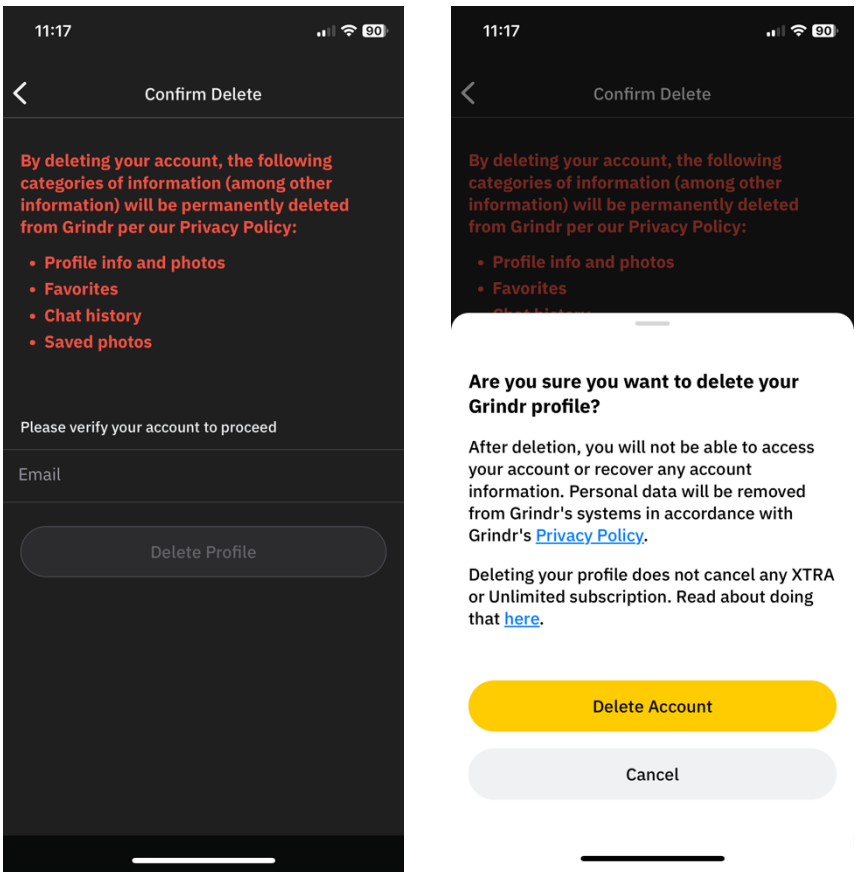
7. Grindr's privacy policy reflects a "commitment to privacy," assuring users that its "goal is to put [them] in control of as much of the Personal Information [they] share with Grindr as possible."[7]

8. Grindr's Privacy Policy states: "If you decide to delete your account, your Personal Information will no longer be made available via the Services and will generally be deleted within 28 days."[8]

9. Grindr states that it discloses users' personal information to a number of third-party providers, but that it only shares HIV status, last tested date, and vaccination status with necessary service providers such as companies that host Grindr's data, process data access requests initiated by users, or send testing reminders to users. Grindr states that it does not disclose health information to advertising companies.[9]

[5] Julie Kvedar, *Back to the Grind: Rethinking Grindr's Accountability for User Content*, 29 S. Cal. Interdisc. L. J. 541 (2020).
[6] *Id*.
[7] *Grindr Privacy and Cookie Policy*, Grindr, https://www.grindr.com/privacy-policy/en-us (last visited Sept. 14, 2023).
[8] *Id*.; *Personal Information We Collect and Data Retention*, Grindr (June 22, 2023), https://www.grindr.com/privacy-policy/personal-information-collected-and-data-retention/en-us.
[9] *How We Share Personal Information*, Grindr (June 22, 2023), https://www.grindr.com/privacy-policy/how-we-may-share/en-us.

10. When users attempt to delete their accounts, the application explicitly tells users, in two separate messages, that their personal data will be permanently deleted from Grindr:




11. Grindr's Data Retention Policy prohibits third-party providers from indefinitely retaining user data.[10]

12. Grindr's Privacy and Cookies Policy requires Grindr to notify users if their data is improperly retained by third parties.[11]

## B. Despite Its Promises to Users, Grindr Has a History of Violating its Users' Privacy and Safety

13. To unlock Grindr's core functionality that allows users to see potential partners in their vicinity, users must share their location data with the app.

14. A 2022 Wall Street Journal article found that Grindr sold location data to ad networks. In one case, the Catholic publication The Pillar bought commercially available location data from a third-party data broker that enabled The Pillar to track individual Grindr usage.

[10] *Personal Information We Collect and Data Retention*, *supra* note 8.
[11] *Grindr Privacy and Cookie Policy*, *supra* note 7.

Using the data, the publication outed a senior official of the U.S. Conference of Catholic Bishops as a user of the app, forcing him to resign.[12]

15. Grindr also collects other types of sensitive data from its users, such as HIV status.

16. In 2018, Grindr came under fire for disclosing users' HIV statuses to third party businesses. It later promised to stop disclosing that information.[13]

17. In 2021, Norway's Data Protection Authority fined Grindr over $7 million for illegally disclosing user data to advertisers.[14]

18. Beyond its mishandling of users' personal data, Grindr has also put user safety at risk by failing to remove abusive and fraudulent profiles.[15]

### C. According to Grindr's Former Chief Privacy Officer, Grindr Knew It Had Committed Multiple Privacy Violations but Failed to Remedy Them

19. From January 2021 until January 2023, Ronald De Jesus served as Grindr's Chief Privacy Officer.[16]

20. In June 2023, De Jesus filed a wrongful termination lawsuit against Grindr alleging that Grindr fired him in retaliation for highlighting Grindr's privacy violations and pushing the company to correct its privacy practices.

21. De Jesus' complaint against Grindr details the company's alleged failure to address multiple privacy violations, including the following:[17]

    a. Even after users delete their accounts, Grindr continues to store user data, including sensitive data like private messages, users' self-reported HIV status,

[12] Byron Tau, *Grindr User Data was Sold Through Ad Networks*, The Wall Street Journal (May. 2, 2022), https://www.wsj.com/articles/grindr-user-data-has-been-for-sale-for-years-11651492800.
[13] Azeen Ghorayshi & Sri Ray, *Grindr is Letting Other Companies See User HIV Status and Location Data*, Buzzfeed News (Apr. 2, 2018), https://www.buzzfeednews.com/article/azeenghorayshi/grindr-hiv-status-privacy.
[14] Terje Solsvik, *Grindr Fine Cut to $7 Mln in Norway Data Privacy Case*, Reuters (Dec 15, 2021), https://www.reuters.com/technology/grindr-fine-cut-7-mln-norway-data-privacy-case-2021-12-15/.
[15] Brief for EPIC, *supra* note 2; Abby Vesoulis, *How Dating Apps Became a Paradise for Predators*, Mother Jones (Sept. & Oct. 2023), https://www.motherjones.com/politics/2023/08/how-dating-apps-became-a-paradise-for-predators/.
[16] Complaint at 1, *De Jesus v. Grindr, LLC*, No. 23STCV13635 (Ca. Super. Ct. Jun. 14, 2023).
[17] *Id.*

vaccination status, sexual preferences, and billions of images, including naked photos;[18]

b. Grindr's retention of user data after users delete their accounts violates Grindr's Data Retention Policy and multiple state privacy laws;[19]

c. Grindr uses OneTrust, a third-party consent management platform, and Amplitude, and third-party data analytics tool; these tools were implemented to enable the collection of user data without user consent;[20]

d. Third-party systems store Grindr users' data indefinitely, and users are not notified about this third-party data retention;[21]

e. Grindr failed to conduct security reviews and audits on its systems containing sensitive user data, including health information like HIV status and vaccination status;[22]

f. Grindr employees and the employees of Grindr's third-party providers have unmonitored access to all Grindr users' personal profiles, including their profiles, email addresses, favorited profiles, messages, and photos;[23] and

g. Grindr allows its ad partners to collect users' personal data immediately after an ad is shown to the user rather than when the user clicks on or interacts with the ad; users are not required to consent nor are allowed to opt-out of this data collection. Because some ads focused on HIV prevention medication, De Jesus indicated that this data collection could be used to identify users who were interested in the medication, implicating sensitive health information.[24]

22. According to De Jesus, Grindr executives were notified about all these privacy violations, but they expressed "disinterest [which] escalated into displeasure and contempt."[25]

23. De Jesus also alleged that Grindr cancelled or halted the privacy-promoting projects he was working on prior to his dismissal, including the production of a privacy video series

[18] *Id*.
[19] *Id* at 9.
[20] *Id* at 8.
[21] *Id* at 11.
[22] *Id* at 13.
[23] *Id* at 13.
[24] *Id* at 14-15.
[25] *Id* at 10.

and the creation of a privacy center, which would have been a central hub for privacy resources on Grindr's website.[26]

24. According to De Jesus' complaint, these privacy violations were still happening with the knowledge of Grindr executives when his wrongful termination suit was filed.[27]

## IV. Legal Analysis

### A. FTC Act

25. Section 5 of the FTC Act prohibits unfair and deceptive acts and practices.[28]

26. A company engages in an unfair trade practice if "the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition." The Commission may consider established public policies along with other evidence.[29]

27. Deceptive practices include material representations, omissions, or practices that are likely to mislead a consumer acting reasonably in the circumstances.[30]

28. In previous actions by the FTC, the Commission has stated that retaining customer data after customers delete their accounts in violation of the company's privacy policy would constitution an unfair or deceptive act or practice in violation of Section 5 of the FTC Act.[31]

29. The Commission has also stated that failing to implement adequate data security practices to safeguard sensitive personal information would constitutes an unfair or deceptive act or practice in violation of Section 5 of the FTC Act.[32]

---

[26] *Id* at 7-8.
[27] *Id*.
[28] 15 U.S.C. § 45.
[29] 15 U.S.C. § 45(n); FTC, Policy Statement on Unfairness (1980), https://www.ftc.gov/legal-library/browse/ftc-policystatement-unfairness.
[30] FTC, Policy Statement on Deception (1983), https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf.
[31] *See, e.g.*, Complaint, *In re Everalbum and Paravision* (May 7, 2021), https://www.ftc.gov/system/files/documents/cases/1923172_-_everalbum_complaint_final.pdf; Complaint for Permanent Injunction and Other Equitable Relief, *In re Ashley Madison* (Dec. 14, 2016), https://www.ftc.gov/system/files/documents/cases/161214ashleymadisoncmplt1.pdf.
[32] *See, e.g.*, Complaint, *In re Chegg, Inc.* (Jan. 26, 2023) https://www.ftc.gov/system/files/ftc_gov/pdf/Chegg-Complaint.pdf; Complaint, *In the Matter of Zoom Video Communications* (Feb. 1, 2021), https://www.ftc.gov/system/files/documents/cases/1923167zoomcomplaint_0.pdf; Complaint, *In re Retina-X Studios, LLC and James N. Johns, Jr.* (Mar 27, 2020), https://www.ftc.gov/system/files/documents/cases/172_3118_retina-x_studios_complaint_0.pdf.

30. Commission statements also make clear that failing to uphold promises made to users in privacy policies constitutes an unfair or deceptive act or practice in violation of Section 5 of the FTC Act.[33]

## B. Health Breach Notification Rule

31. The FTC issued the Health Breach Notification Rule (HBNR) on August 25, 2009.[34] Congress directed the FTC to issue the HBNR through the American Recovery and Reinvestment Act of 2009. The HBNR requires certain web-based businesses not covered by HIPAA to notify consumers when the security of their electronic health information is breached.[35]

32. The HBNR applies to vendors of personal health records (PHR), PHR related entities, and third-party service providers.[36]

33. The HBNR defines a PHR related entity as an entity, other than a HIPAA-covered entity, that "(1) Offers products or services through the Web site of a vendor of personal health records; (2) Offers products or services through the Web sites of HIPAA-covered entities that offer individuals personal health records; or (3) Accesses information in a personal health record or sends information to a personal health record."[37]

34. The HBNR defines a third-party service provider as an entity that "(1) Provides services to a vendor of personal health records in connection with the offering or maintenance of a personal health record or to a PHR related entity in connection with a product or service offered by that entity; and (2) Accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured PHR identifiable health information as a result of such services."[38]

35. The HBNR requires covered entities to notify consumers when a breach of security of a personal health record (PHR) is discovered. PHR is "an electronic record of PHR identifiable health information on an individual that can be drawn from multiple sources and that is managed, shared, and controlled by or primarily for the individual."[39] The PHR must be PHR identifiable health information, meaning information that is provided by or on behalf of an individual and can be used to identify the individual.[40]

---

[33] *See, e.g.*, Complaint, *In re Flo Health, Inc.* (Jun. 22, 2021), https://www.ftc.gov/system/files/documents/cases/192_3133_flo_health_complaint.pdf; Complaint of Commissioners Simons, Phillips, Chopra, Slaughter, & Wilson, *In the Matter of Zoom Video Communications* (Feb. 1, 2021), https://www.ftc.gov/system/files/documents/cases/1923167zoomcomplaint_0.pdf.
[34] 16 C.F.R. § 318.
[35] *FTC Issues Final Breach Notification Rule for Electronic Health Information*, FTC (Aug. 17, 2009), https://www.ftc.gov/news-events/news/press-releases/2009/08/ftc-issues-final-breach-notification-rule-electronic-health-information.
[36] 16 C.F.R. § 318.2.
[37] 16 C.F.R. § 318.2(f).
[38] 16 C.F.R. § 318.2(h).
[39] 16 C.F.R. § 318.2(d).
[40] 16 C.F.R. § 318.2(e).

36. Following the discovery of a breach of security of unsecured PHR identifiable health information, a covered entity must notify each individual who is a citizen or resident of the United States that their PHR identifiable health information was acquired by an unauthorized person and notify the FTC.[41] All notifications must be sent no later than 60 days after the discovery of the security breach.[42]

## V. Grindr's Apparent Violations of the FTC Act

### A. Grindr's Unfair Retention and Disclosure of User Data Constitutes a Violation of the FTC Act

37. Grindr's apparent personal data practices—including its alleged retention and disclosure of user data, its apparent failure to implement adequate data security practices, and its alleged failure to control employee access to user data[43]—are unfair because they cause or are likely to cause substantial injury to consumers which is not reasonably avoidable by consumers and because they are not outweighed by countervailing benefits.[44]

38. Grindr's apparent personal data practices have caused or are likely to cause substantial injury to its users and former users because they expose users to security breaches of highly sensitive data, including health information like HIV status and vaccination status; other information users include on their profiles like sexual preference and age; users' app usage; and location data.

39. Grindr's alleged failure to enforce its own privacy policies exposes users to security breaches of its own systems as well as breaches of third-party systems.

40. Consumers cannot reasonably avoid the harm Grindr allegedly imposes when it retains and discloses user data in violation of Grindr's policies. Grindr users reasonably rely on the promises Grindr makes in its policies because Grindr users must agree to these policies when creating a Grindr account.

41. Further, Grindr apparently failed to notify users that it retained and disclosed user data in violation of its policies. Even if Grindr had notified users of a breach, users have little power to take their own protective measures to secure their data.

42. The misuse of user data by Grindr outlined in De Jesus' complaint is not outweighed by countervailing benefits to consumers or competition. Grindr users have allegedly been exposed to security breaches because of Grindr's practices, and users whose data was breached after they deleted their accounts could not take part in any possible benefits because they are no longer using Grindr's app.

---

[41] 16 C.F.R. § 318.3.
[42] 16 C.F.R. § 318.4(a).
[43] Complaint, *supra* note 16.
[44] 15 U.S.C. § 45(n); Policy Statement on Unfairness, *supra* note 29.

## B. Grindr's Deceptive Retention and Disclosure of User Data Constitutes a Violation of the FTC Act

43. Grindr's alleged privacy practices described in De Jesus' complaint—including its retention and disclosure of user data, its apparent failure to implement adequate data security practices, and its alleged failure to control employee access to user data,[45] in violation of the company's privacy policy—are deceptive because the company made "material representations, omissions, or practices that are likely to mislead a consumer acting reasonably in the circumstances." [46]

44. Grindr allegedly made representations to users through its privacy policies that it would delete user data after the user deleted their account and that it would not permit third parties to indefinitely retain user data.

45. De Jesus' complaint alleges that, in practice, Grindr failed to delete user data from its own systems after users deleted their accounts. Additionally, third-party providers were permitted to retain user data indefinitely, and Grindr did not ensure that personal information from deleted accounts was removed from third-party providers' systems.

46. These representations are material because Grindr's alleged privacy practices are likely to affect a consumer's decision regarding whether to use Grindr.[47] As described above, Grindr allegedly collects and stores sensitive data from users, including information about users' sexual preferences, self-reported HIV status, chat history with matches, photos users send and receive on the app (including nude images), and location information.[48] Grindr promises to give users control over their personal information and to delete users' information when users delete their accounts.[49] Learning that Grindr breaks the promises it makes to users would likely affect a consumer's decision regarding whether to use Grindr.

47. Users were likely to be misled by Grindr's privacy policies because Grindr does not share its actual data retention and disclosure practices with its users. As former Chief Privacy Officer, De Jesus had access to information about Grindr's business practices, which apparently demonstrates Grindr's failure to fulfill the terms of the company's own privacy policies. However, users and former users have no way of determining whether their data is improperly disclosed or retained unless the company notifies users.

48. Grindr users reasonably relied on Grindr's representations; these promises were explicitly stated in Grindr's Privacy and Cookie Policy and Grindr's Data Retention Policy.[50]

---

[45] Complaint, *supra* note 16.
[46] 16 C.F.R. § 318.
[47] Policy Statement on Deception, *supra* note 30.
[48] Complaint, *supra* note 16.
[49] *Grindr Privacy and Cookie Policy*, *supra* note 7; *Personal Information We Collect and Data Retention*, *supra* note 8.
[50] *Id*.

## VI. Grindr's Apparent Violations of the HBNR

49. Grindr is subject to the HBNR because it is a PHR related entity. Grindr "accesses information in a personal health record"[51] when it prompts users to self-report PHR like their HIV status, last tested date, and vaccination status.[52]

50. Self-reported HIV and vaccination statuses fulfill the HBNR's definition of PHR because the data is stored electronically, the data is linked to individual and identifiable profiles, Grindr allegedly draws information from users from multiple sources (including user inputs, app usage, browser history, etc.), and users share their own data by self-reporting the health information.[53]

51. De Jesus' complaint alleges that he notified Grindr that third-party providers retained access to user data after users had deleted their accounts in violation of Grindr's privacy policies.

52. As alleged in De Jesus' complaint, the third-party providers had proper authority to possess user data while user accounts were active, but the third-party providers' possession of the data became improper once users deleted their accounts. Grindr apparently failed to ensure that its agreements with users—the Grindr Privacy and Cookie Policy and the Data Retention Policy—were upheld, resulting in a security breach of PHR.

53. Further, Grindr also breached the HBNR by allegedly retaining user health data after users effectively revoked their consent for Grindr to retain such data by deleting their Grindr accounts, in accordance with the Grindr Data Retention Policy.

54. After De Jesus notified executives at Grindr of the security breach, Grindr allegedly failed to notify users of the security breach pursuant to the HBNR.

## VII. Prayer for Relief

55. EPIC urges the Federal Trade Commission to begin an investigation of Grindr LLC to determine if Grindr, through its handling of users' personal data, has engaged in unfair and deceptive trade practices under Section 5 of the FTC Act and violations of the Health Breach Notification Rule. At a minimum, the FTC should investigate to what extent Grindr engages in the following practices:

    a. Retaining user data after users delete their Grindr accounts, including account data, messages, and photos sent and received via Grindr's platform;

[51] 16 C.F.R. § 318.2(f)(3).
[52] 16 C.F.R. § 318.2.
[53] 16 C.F.R. § 318.2(e).

b. Permitting third party service providers to retain user data or health information after users deleted their Grindr accounts;

c. Disclosing user data with third parties without user consent;

d. Failing to maintain adequate data security practices to safeguard user data;

e. Permitting employees to gain unmonitored access to Grindr users' account data;

f. Enabling advertisers to obtain user data without consent and/or in violation of Grindr's privacy policy;

g. Retaining health information after users delete their Grindr accounts, including HIV status, vaccination status, and last tested date; and

h. Failing to notify users that their health information has been breached by Grindr or any third parties in violation of the HBNR.

56. EPIC furthers urges the Commission to:

a. Halt any unlawful or impermissible retention and disclosure of personal user data by Grindr;

b. Require that Grindr notify any users whose data has been improperly disclosed or retained in violation the HBNR;

c. Issue an injunction requiring that Grindr implement and maintain an effective data security program;

d. Require Grindr LLC to comply with the Health Breach Notification Act;

e. Impose penalties pursuant to the HBNR for any failure by Grindr to notify users that their PHR was breached; and

f. Provide such other relief as the Commission finds necessary and appropriate.

Respectfully Submitted,

*/s/ John Davisson*
John Davisson
Director of Litigation
davisson@epic.org

*/s/ Caroline Kraczon*
Caroline Kraczon
Law Fellow
kraczon@epic.org

ELECTRONIC PRIVACY
INFORMATION CENTER (EPIC)
1519 New Hampshire Ave. NW
Washington, DC 20036
202-483-1140 (tel)
202-483-1248 (fax)