

United States Senate

WASHINGTON, DC 20510

September 24, 2025

Spencer Rascoff
Chief Executive Officer
Match Group, Inc.
8750 North Central Expressway
Dallas, TX 75231

Dear Mr. Rascoff:

Given Match Group’s stated commitment to improving upon its historical practices relating to user safety,¹ we write today to request documents and information about the company’s policies, procedures, and practices related to fraudulent activity on its platforms.² Romance scams, in which fraudsters form relationships to induce money or gifts from victims, have become a leading form of financial fraud in the United States, with annual losses reaching at least \$1.3 billion, according to the Federal Trade Commission (FTC).³ Independent research indicates that nearly half of all online dating users in the United States have used a Match Group platform, and more than half of all users believe they have encountered a scammer.⁴ On a recent earnings call, you stated that Match Group would improve trust and safety and “prioritize users over short-term revenue and profit,” marking a shift from the way the company “operated historically.”⁵

Over the years, many events have raised questions about whether Match Group—in its business practices and algorithmic design—has contributed to the proliferation of romance scams online. In a 2019 complaint, FTC alleged that Match Group knowingly exposed users to fraud.⁶ In fact, FTC alleged that between 2013 and mid-2018, up to 30 percent of new Match.com members were scammers.⁷ FTC further alleged that Match.com sent mass emails to non-paying users promoting paywalled communications from accounts it suspected or knew were fraudulent.⁸ This led nearly 500,000 users to subscribe within 24 hours of receiving an email or other advertisement that involved a fraudulent communication.⁹ These allegations raise concerns about whether and how Match Group protects users from fraud on its platforms.

¹ *Dating Apps Have Hit a Wall. Can They Turn Things Around?*, The New York Times (Mar. 12, 2024) (www.nytimes.com/2024/03/12/business/dating-apps-tinder-bumble.html).

² For the purposes of this letter and its requests, a Match Group “platform” refers to Tinder, Hinge, Match (formerly known as Match.com), Plenty of Fish, and OkCupid.

³ Federal Trade Commission, *Romance Scammers’ Favorite Lies Exposed* (Feb. 9, 2023) (www.ftc.gov/news-events/data-visualizations/data-spotlight/2023/02/romance-scammers-favorite-lies-exposed).

⁴ Pew Research Center, *From Looking for Love to Swiping the Field: Online Dating in the U.S.* (Feb. 2, 2023) (www.pewresearch.org/wp-content/uploads/sites/20/2023/01/PI_2023.02.02_Online-Dating_FINAL.pdf).

⁵ Match Group, Inc., Q1 2025 Earnings Call Transcript (seekingalpha.com/article/4783795-match-group-inc-mtch-q1-2025-earnings-call-transcript).

⁶ Complaint, *Federal Trade Commission v. Match Group, Inc.*, No. 3:19-cv-02281 (N.D. Tex. Sep. 25, 2019).

⁷ *Id.*

⁸ *Id.*

⁹ *Id.*

Match Group has stated that it “permanently discontinued” the above practices.¹⁰ Publicly and privately, however, individuals who have worked at Match Group have suggested that “[rooting out scammers] wasn’t a real priority backed up by resources”¹¹ and that the company’s “obsession with metrics ... [is] potentially dangerous.”¹² At a recent panel appearance, Match Group’s Head of Trust and Safety, Yoel Roth, acknowledged that organized criminal groups increasingly carry out romance fraud in technologically sophisticated overseas scam compounds.¹³ Mr. Roth also said that Tinder’s “selfie-verification” process—whereby users create and verify their own accounts—is “pretty simple for a human to pass,” and that Match Group had seen thousands of submissions with similar backgrounds, likely originating from a scam compound.¹⁴ One expert has warned that the process offers “no guarantee against [deceptive profiles] because the images used for verification ... need not be the ones used on a person’s dating profile.”¹⁵ These statements appear consistent with the experiences of many online dating users. According to a 2023 Pew Research Center survey, for example, users are more than three times as likely to rate online dating companies as “very bad” instead of “very good” at removing fake accounts.¹⁶

We are also concerned that Match Group, through its algorithmic design, creates trust that romance scammers can exploit. According to former OkCupid CEO Christian Rudder, for example, “users sent more first messages when we said they were compatible...[e]ven when they should be wrong for each other.”¹⁷ Studies also suggest that increased platform use may foster greater trust in dating algorithms.¹⁸ As a result, a persuasive algorithmic design may help facilitate romance scams when it recommends fraudsters who benefit from users’ trust in the platform’s judgments of compatibility.

Match Group’s business model is to keep users engaged, but this engagement is dangerous when it involves scammers. Online dating platforms drive user engagement, in part, with the promise of connections based on compatibility. Tinder, for instance, represents that its algorithm can “pick better potential matches” and helps users “see people they’ll vibe with.”¹⁹ Expert research into romance scams, however, has identified recurring characteristics and patterns among

¹⁰ Match Group, Inc.’s Motion to Dismiss and Brief in Support (Oct. 17, 2019), *Federal Trade Commission v. Match Group, Inc.* N.D. Tex. (No. 3:19 CV 02281).

¹¹ As *Romance Scammers Turn Dating Apps Into “Hunting Grounds,” Critics Look to Match Group to Do More*, CBS News (Apr. 24, 2024) (www.cbsnews.com/news/romance-scams-dating-apps-investigators-match-group/).

¹² Markup, *Dating App Cover-Up: How Tinder, Hinge, and Their Corporate Owner Keep Rape under Wraps* (Feb. 13, 2025) (themarkup.org/investigations/2025/02/13/dating-app-tinder-hinge-cover-up).

¹³ Vice President of Trust & Safety Yoel Roth, Match Group, Remarks at Tech-Wide Battle Against Online Fraud SXSW 2025 (Mar. 10, 2025) (schedule.sxsw.com/2025/events/PP153022).

¹⁴ *Id.*

¹⁵ Irina D. Manta, *Tinder Backgrounds*, Georgia Law Review (forthcoming) (Apr. 16, 2025).

¹⁶ Pew Research Center, *From Looking for Love to Swiping the Field: Online Dating in the U.S.* (Feb. 2, 2023) (www.pewresearch.org/wp-content/uploads/sites/20/2023/01/PI_2023.02.02_Online-Dating_FINAL.pdf).

¹⁷ Christian Rudder, *We Experiment on Human Beings!*, OkCupid (blog) (July 28, 2014) (web.archive.org/web/20140802000357/http://blog.okcupid.com/index.php/we-experiment-on-human-beings).

¹⁸ See e.g., Alice Binder et al., *Dating Algorithms? Investigating the Reciprocal Relationships Between Partner Choice FOMO, Decision Fatigue, Excessive Swiping, and Trust in Algorithms on Dating Apps*, New Media & Society (Oct. 12, 2024) and Junwen Hu and Rui Wang, *Familiarity Breeds Trust? The Relationship Between Dating App Use and Trust in Dating Algorithms via Algorithm Awareness and Critical Algorithm Perceptions*, International Journal of Human-Computer Interaction (May 31, 2023).

¹⁹ *Tinder, Powering Tinder – The Method Behind Our Matching* (www.help.tinder.com/hc/en-us/articles/7606685697037-Powering-Tinder-The-Method-Behind-Our-Matching).

perpetrators and victims. Scammers often quickly escalate emotional intimacy (often termed “love bombing”),²⁰ to which users prone to romantic idealization are especially vulnerable.²¹ These interactions can generate engagement metrics—such as high positive reply rates and low negative reply rates—that algorithms may interpret as indicators of compatibility.²² As one study on machine learning systems noted, “vulnerabilities can be automatically exploited when the vulnerable state or condition of an individual becomes entangled with the optimization criteria of an algorithmic system.”²³ In that context, Match Group’s ability to monitor and influence user behavior, paired with limited transparency about potential harmful outcomes,²⁴ raises concerns that its platforms may, even inadvertently, create conditions where romance scams are more likely to begin.

To aid Congress in understanding Match Group’s efforts to prevent romance scams and the factors that allow these scams to begin on its platforms, please provide responses to the following document and information requests. These requests cover the time period of January 1, 2022, to the present, unless otherwise specified. Please provide your responses no later than October 15, 2025.

1. A description of the “signals”²⁵ associated with accounts suspected or known to be fraudulent or scammers and how Match Group accounts for these signals in detection systems, recommendation algorithms, and the Trust and Safety team’s fraud review process;
2. All policies and procedures concerning the detection, review, and removal of accounts suspected or known to be fraudulent or scammers; their algorithmic treatment; and any restrictions on their visibility or communication with other users;
3. For any accounts suspected or known to be fraudulent or scammers, documents sufficient to show for each quarter:

²⁰ Fangzhou Wang and Volkan Topalli, *Understanding Romance Scammers Through the Lens of Their Victims: Qualitative Modeling of Risk and Protective Factors in the Online Context*, American Journal of Criminal Justice (Nov. 16, 2022) and Simon Moseley, *Automating Deception: AI’s Evolving Role in Romance Fraud*, CETaS Briefing Papers (Apr. 2025).

²¹ Monica T Whitty and Tom Buchanan, *The Online Dating Romance Scam: Causes and Consequences of Victimhood*, Psychology, Crime & Law (Mar. 28, 2013).

²² In 2016, Match Group was granted a patent for a recommendation system based on “indicators of relevance.” These include the number and duration of messages exchanged between matched users. The system correlates these indicators with the users’ attributes and uses those attributes as proxies to predict the relevance (i.e., compatibility) of future matches. U.S. Patent No. 9,449,282 B2 (issued Sep. 20, 2016). *See also*, Luiz Augusto Pizzato, et al., *The Effect of Suspicious Profiles on People Recommenders*, User Modeling, Adaptation and Personalization: 20th International Conference (July 2012) (applying online dating platform data and finding that certain reciprocal recommender algorithms favored fraudulent users, “who have a distinctive behavior of always replying positively to people”); Bao Kham Chau, *Engineering a Fiduciary: Expanding the Regulatory Scope of Algorithmic Bias*, Harvard Journal of Law & Technology (2024).

²³ Inga Strümke et al., *Against Algorithmic Exploitation of Human Vulnerabilities*, arXiv (preprint) (Jan. 12, 2023).

²⁴ The Markup, *Dating App Cover-Up: How Tinder, Hinge, and Their Corporate Owner Keep Rape under Wraps* (Feb. 13, 2025) (themarkup.org/investigations/2025/02/13/dating-app-tinder-hinge-cover-up).

²⁵ Mr. Roth has stated that his “team is keeping an eye out for signals of scams.” Vice President of Trust & Safety Yoel Roth, Match Group, Remarks at Tech-Wide Battle Against Online Fraud SXSW 2025 (Mar. 10, 2025) (schedule.sxsw.com/2025/events/PP153022).

- a. The number of these accounts, whether they were removed, and their geographic distribution;
 - b. Median time between account creation and (1) detection and (2) removal, broken down by detection method (e.g., user reports, manual review, automatic review, etc.) and “signal” (e.g., false identity, automated behavior, behavioral or language patterns, etc.);
 - c. The number of accounts detected but not removed within 24 hours, broken down by reason for non-removal (e.g., insufficient evidence, user remediation, process delay, false positive, etc.);
 - d. Total number of user messages sent and received; total number of “matches” (or platform equivalent); total session duration in which users interacted with these accounts; and aggregations of any other metrics used to evaluate engagement, profile quality, and “matching” outcomes; and
 - e. Platform revenues from in-app purchases by these accounts and users who liked, matched, or messaged (or platform equivalents) with these accounts within 24 hours before purchase;
4. Memoranda, presentations, reports, studies, analyses, audits, and meeting notes referring or relating to the algorithmic recommendation of accounts suspected or known to be fraudulent or scammers;
 5. All internal reports, studies, or analyses referring or relating to the specific attributes,²⁶ including demographics, platform use, and off-platform behavior, of:
 - a. Accounts suspected or known to be fraudulent or scammers; and
 - b. Users targeted by or interacting with accounts suspected or known to be fraudulent or scammers;
 6. All documents and communications concerning the design, development, effectiveness, or consideration of fraud prevention measures, including measures discontinued or not implemented;
 7. Itemized quarterly investments in trust and safety, including but not limited to the following categories:
 - a. Trust and safety policy, operations, and data;
 - b. Social advocacy;
 - c. Law enforcement operations and outreach;
 - d. Platform safety services and features; and
 - e. Safety by design;²⁷

²⁶ “Attributes” includes but is not limited to a user’s “preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.” Tinder, CCPA Privacy Notice Addendum (<https://policies.tinder.com/ccpa-addendum/intl/en/>) (accessed June 5, 2025).

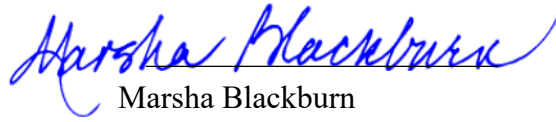
²⁷ Match Group’s Impact Report 2024 states that the company’s safety strategies “target five key pillars:” trust and safety policy, operations, and data; social advocacy; law enforcement operations and outreach; platform safety services and features; and safety by design. Match Group, *Match Group Impact Report 2024* (Apr. 23, 2024) (sustainabilityreports.com/reports/match-group-inc-2024-impact-report-pdf/).

8. Itemized quarterly budget proposals, approved budgets, and staffing levels for Trust and Safety teams, including both employees and contractors and broken down by geographic area of responsibility, if applicable; and
9. Any document productions referring or relating to the issues outlined above made since September 1, 2019, to the U.S. Federal Trade Commission, the U.S. Department of Justice, state attorneys general, any committee or subcommittee of the U.S. Congress, or any U.S. Attorney's office.

Sincerely,



Margaret Wood Hassan
Ranking Member
U.S. Congress Joint Economic
Committee



Marsha Blackburn
Chairman
Subcommittee on Consumer Protection,
Technology, and Data Privacy

cc: David Schweikert
Chairman, Joint Economic Committee

Eric Schmitt
Vice Chairman, Joint Economic Committee