BRETT A. SHUMATE
Assistant Attorney General, Civil Division
JORDAN C. CAMPBELL
Deputy Assistant Attorney General
SARMAD M. KHOJASTEH
Senior Counsel
LISA K. HSIAO
Acting Director, Consumer Protection Branch
ZACHARY A. DIETERT
Assistant Director
MARCUS P. SMITH
Trial Attorney
Consumer Protection Branch
Civil Division, U.S. Department of Justice
450 5th Street, NW, Suite 6400-South
Washington, DC 20001
Telephone: (202) 353-9712 (Smith)

UNITED STATES DISTRICT COURT

FOR THE CENTRAL DISTRICT OF CALIFORNIA

UNITED STATES OF AMERICA, Plaintiff, v. ICONIC HEARTS HOLDINGS, INC., a corporation; and HUNTER RICE, individually and as an officer of ICONIC HEARTS HOLDINGS, INC., Defendants.	Case No. 2:25-CV-9310 **COMPLAINT FOR PERMANENT INJUNCTION, MONETARY JUDGMENT, CIVIL PENALTY JUDGMENT, AND OTHER RELIEF** **DEMAND FOR JURY TRIAL**

Plaintiff, the United States of America, acting upon notification and referral from the Federal Trade Commission ("FTC"), for its Complaint alleges:

SUMMARY OF CASE

1. Defendant Iconic Hearts Holdings, Inc. ("Iconic Hearts") and its founder, CEO, and sole Director, Defendant Hunter Rice (collectively, "Defendants"), are the developers of the "sendit - get it now" ("Sendit") mobile application ("app"), a social media messaging app designed for children and young teenagers.

2. Defendants trick Sendit users into believing they have received provocative and sometimes sexual or romantic messages from their social media contacts, when in reality it is often Defendants themselves who sent those messages.

3. Defendants profit from their deception by luring young users into paid subscriptions to find out who sent these messages. Defendants do not clearly or conspicuously disclose the terms and features of the subscriptions, including that they automatically renew on a weekly basis and continue charging the user until they are cancelled.

4. Defendants also fail to fulfill their promises to subscribers. They instead provide subscribers only vague and sometimes entirely fabricated information about a message's purported sender. For messages that were sent by a user's actual contacts, Defendants have charged users yet another fee before revealing the sender's identity.

5. Defendants have also knowingly and unlawfully collected personal information from numerous children under the age of 13, without informing parents or obtaining their consent.

6. Plaintiff brings this action for Defendants' violations of the Children's Online Privacy Protection Rule ("COPPA Rule"), 16 C.F.R. § 312, the Restore Online Shoppers' Confidence Act ("ROSCA"), 15 U.S.C. §§ 8401-05, and Section

5(a) of the FTC Act, 15 U.S.C. § 45(a). For these violations, Plaintiff seeks relief, including a permanent injunction, monetary relief, civil penalties, and other relief pursuant to Sections 5(m)(1)(A), 13(b), and 19 of the FTC Act, 15 U.S.C. §§ 45(m)(1)(A), 53(b) and 57b, Sections 1303(c) and 1306(d) of the Children's Online Privacy Protection Act of 1998 ("COPPA"), 15 U.S.C. §§ 6502(c) and 6505(d), the COPPA Rule, and Section 5 of ROSCA, 15 U.S.C. § 8404.

JURISDICTION AND VENUE

7. This Court has subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331, 1337(a), 1345, and 1355.

8. Venue is proper in this District under 28 U.S.C. §§ 1391(b)(1), (b)(2), (b)(3), (c)(2), and (d), 1395(a), and 15 U.S.C. § 53(b).

PLAINTIFF

9. Plaintiff is the United States of America. Plaintiff brings this action upon notification and referral from the FTC, pursuant to Section 16(a)(1) of the FTC Act, 15 U.S.C. § 56(a)(1).

DEFENDANTS

10. Defendant Iconic Hearts is a Delaware corporation with its principal place of business at 1639 Eleventh Street, Suite 226, Santa Monica, CA, 90404. Iconic Hearts is engaged in the business of developing social networking applications. Iconic Hearts transacts or has transacted business in this District and throughout the United States.

11. Defendant Hunter Rice is the founder, CEO, and sole Director of Iconic Hearts. At all times relevant to this Complaint, acting alone or in concert with others, he has formulated, directed, controlled, had the authority to control, or participated in the acts and practices of Iconic Hearts described in this Complaint. Rice founded and incorporated Iconic Hearts, invented and designed Sendit, is the company's Chief Executive Officer, and directed the company and its employees and independent contractors with regard to the conduct alleged herein. Rice was

the company's exclusive point of contact for the Apple App Store regarding the launch, features, revisions, and functionalities of Sendit. Rice knew that Iconic Hearts was collecting personal information from children under the age of 13 on Sendit and was aware of complaints Iconic Hearts received regarding fake messages and unfair purchases on Sendit. Rice resides in this District and, in connection with the matters alleged herein, transacts or has transacted business in this District and throughout the United States.

COMMERCE

12. At all times relevant to this Complaint, Defendants have maintained a substantial course of trade in or affecting commerce, as "commerce" is defined in Section 4 of the FTC Act, 15 U.S.C. § 44.

DEFENDANTS' BUSINESS ACTIVITIES

Defendants Design and Launch the Sendit Mobile Application, Directing it to Children and Teenagers

13. Defendants are the developers, marketers, and distributors of Sendit, an anonymous messaging app designed for use on social networking platforms like Snapchat, X (formerly known as Twitter), and Instagram. Iconic Hearts launched Sendit on or about November 9, 2018, in the Apple App Store. Sendit has also been available through the Google Play Store since around May 16, 2020. In 2020, downloads of Sendit regularly exceeded 1,000 per day. By mid-2021, downloads of Sendit were regularly exceeding 10,000-20,000 per day.

14. Defendants advertise Sendit as a forum for users to interact with their friends on social media through anonymous messages. For example, at all times, Sendit's pages on the Google Play and Apple app stores have described the app as a service through which users share a prompt that their friends answer through responses delivered by Sendit.

15. Sendit provides a list of "prompts" that invite anonymous responses from their social media contacts. Once users choose a prompt that they want to

share with their contacts, Sendit generates a personalized link that users can post to their social media accounts. Over time, the Defendants have made available an increasing number of Sendit prompts for users to share.

16. Users' social media contacts can provide an anonymous response to the prompt by clicking on the personalized link and responding to the prompt. Sendit conceals the senders' identifying information—their Snapchat "avatars" or display names, for example—to anonymize their messages. Sendit then makes the anonymous message available for the recipients to review in their Sendit inbox. Below are images capturing an example of this process in November 2023:

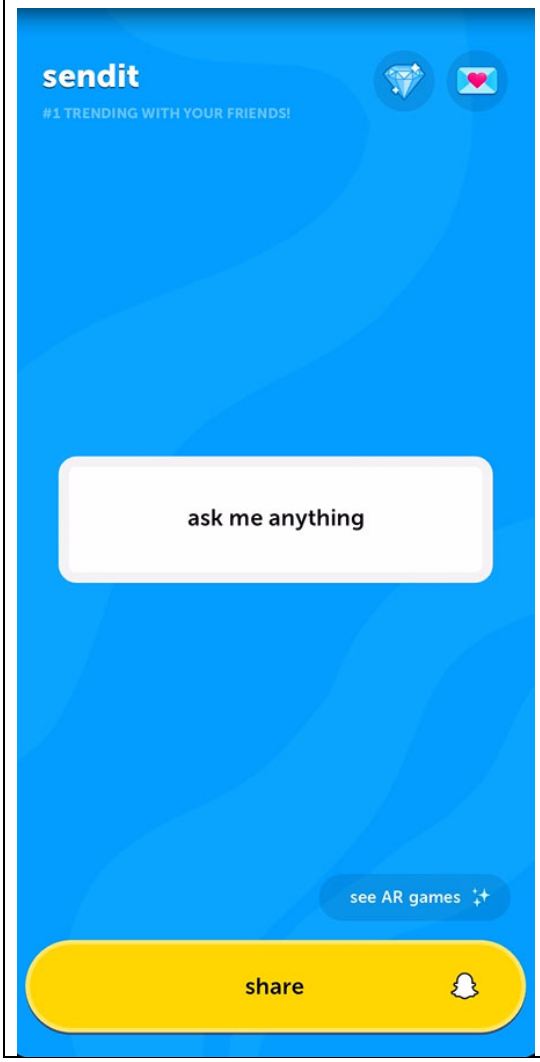
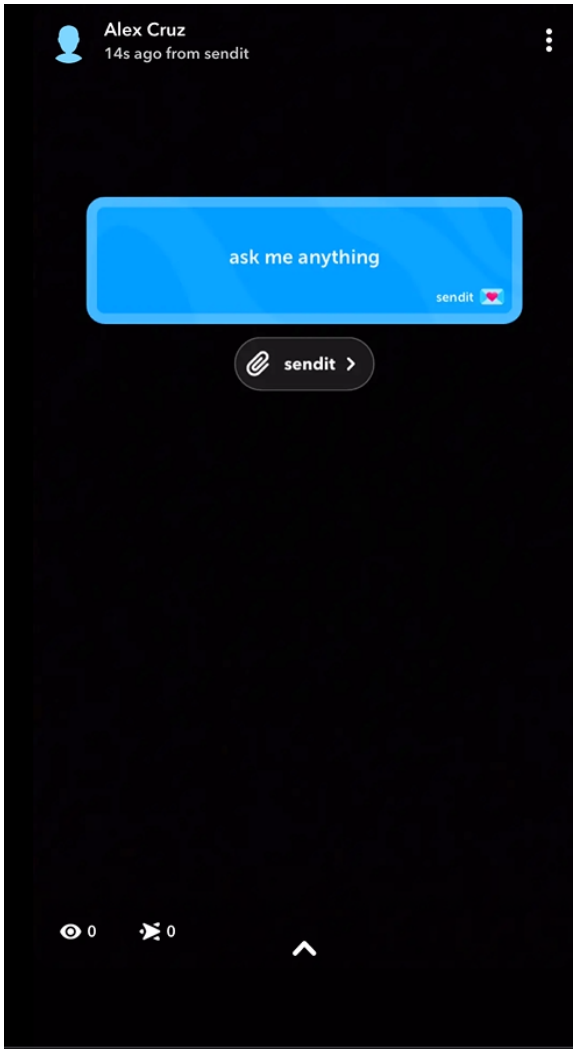
Image 1: User Selects a Prompt on Sendit & Creates a Personalized Link to Post to Social Media	Image 2: User Posts the Prompt & Link to Social Media (e.g., Snapchat)
	

Image 3: User Receives Responses to their Prompts as Messages in Their Sendit Inbox	Image 4: User Opens Messages in Sendit Inbox and Sees Anonymous Responses
	

17. Numerous Sendit users are under the age of 18. Defendant Rice designed Sendit with input from a 13-year-old relative to resemble the "never have

I ever" or "truth or dare" party games that were popular with the relative's middle-school friends. Upon creation of Sendit, Rice contacted his relative's 13- and 14-year-old friends to encourage them to use Sendit, and the relative further helped the app become popular by sharing it himself among his middle-school classmates. In late 2022, Defendants selected and paid several teen influencers to promote the app, many of whom described their day-to-day experiences in high school on their social media. Defendants have also maintained a "schools" function on the Sendit profile page, in which users can search for and find their school to put on their Sendit profile and find fellow users at that school. A user can pick their school from a list of local schools that include elementary, middle, and high schools. Defendants have also continuously offered a prominent page for "parents" on the various versions of the Sendit website, given the high proportion of Sendit users under the age of 18.

18. Defendants have stated that Sendit may be downloaded and used by children under the age of 13. For example, the Sendit website has at times explicitly stated that the app is for users as young as 12 and that Iconic Hearts is "on a mission to become the primary destination where every social interaction for gen alpha can happen." Since at least as early as January 2024, Defendants have described Sendit as a "Gen Alpha social networking app." Gen Alpha is commonly understood to comprise people born no earlier than 2010, who were no older than 13 at the start of 2024. In response to inquiries from parents and children, Defendant Iconic Hearts informed many parents that Sendit is for users 12 and up.

Defendants Knowingly Collect Personal Information from Children Under 13, Without Notifying Parents or Obtaining Parental Consent

19. In numerous instances since 2018, Defendants have had actual knowledge of their collection, storage, and maintenance of personal information from children under 13. For example, in 2022, over 116,000 users reported their age as under 13 while using a date-of-birth profile function on Sendit. Defendants

also repeatedly receive complaints from parents and children that explicitly reference the child's age as being under 13.

20. Defendants have collected, stored, or maintained personal information from these children and all Sendit users, including but not limited to users' names, contacts, phone numbers, location data, birthdates, photos, and identifying usernames on various social media profiles—including, but not limited to, Instagram, TikTok, YouTube, Snapchat, X (formerly known as Twitter), Twitch, and BeReal.

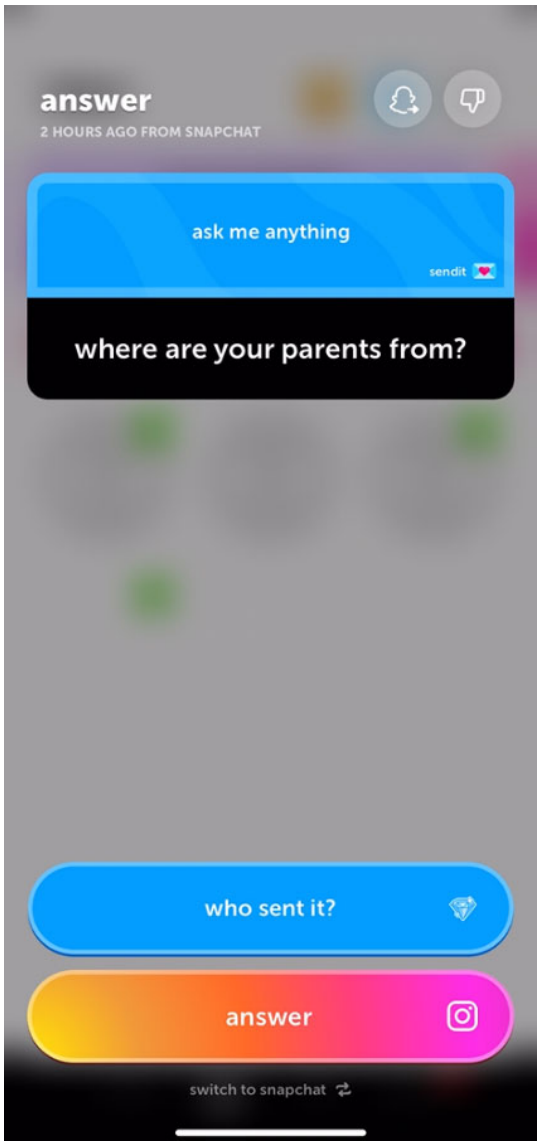
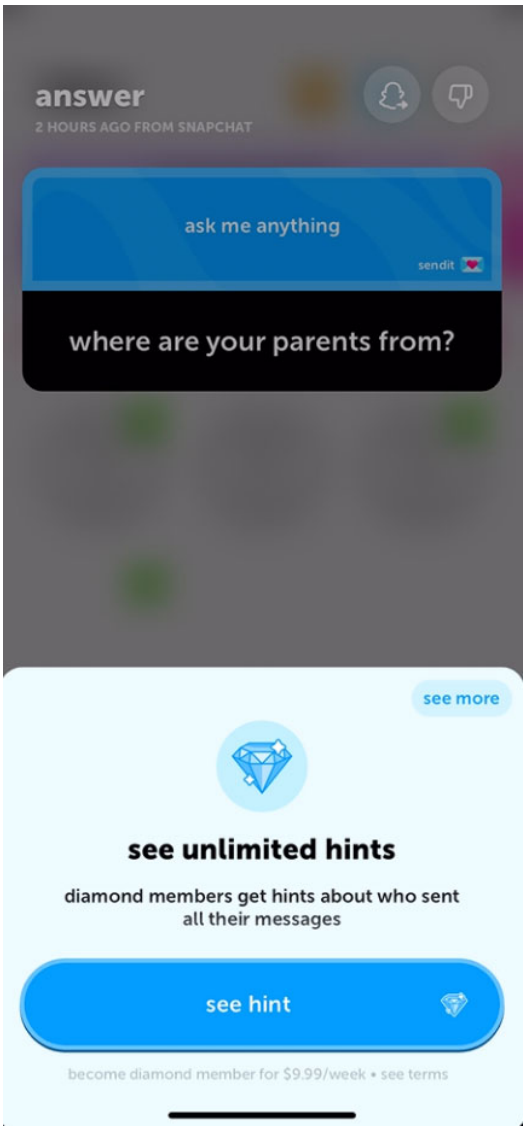
21. Defendants have collected this personal information from children under 13 without complying with COPPA. Defendants have not provided notice to the parents of children under the age of 13 regarding the data that they collect, store, and maintain. Nor have Defendants obtained verifiable parental consent from the parents of children who use the app.

Defendants Offer the Diamond Membership, Which Promises to Reveal the Identity of the Senders of Anonymous Messages

22. Users are not charged for downloading Sendit on the Apple App Store or Google Play Store, nor are they charged when they share a Sendit prompt with their social media contacts. Rather, Sendit monetizes its app by offering a subscription, the "Diamond Membership," to Sendit message recipients who want to find out their anonymous message senders' identities. Since 2019, Iconic Hearts has offered the Diamond Membership, an in-app purchase on Sendit, often for a price of $8.99 or $9.99 per week. The Diamond Membership is automatically renewed on a weekly basis until canceled by the consumer, and thus constitutes a sales transaction with a negative option feature, as defined in Paragraph 77 below.

23. Since approximately 2021, when Defendants first began offering the Diamond Membership, they have promoted it as a service that reveals the senders of anonymous messages the consumer receives. For example, until around June 2024, a consumer reviewing an anonymous message would see a screen that

contained a "who sent it?" call-to-action button, inviting the consumer to learn the sender's identity (Image 5). Clicking on the "who sent it?" button generated a pop-up screen that read, "see unlimited hints – diamond members get hints about who sent all their messages," which also included a "see hint" call-to-action button inviting the consumer to sign up for Diamond Membership (Image 6) as shown in the example illustrations below:

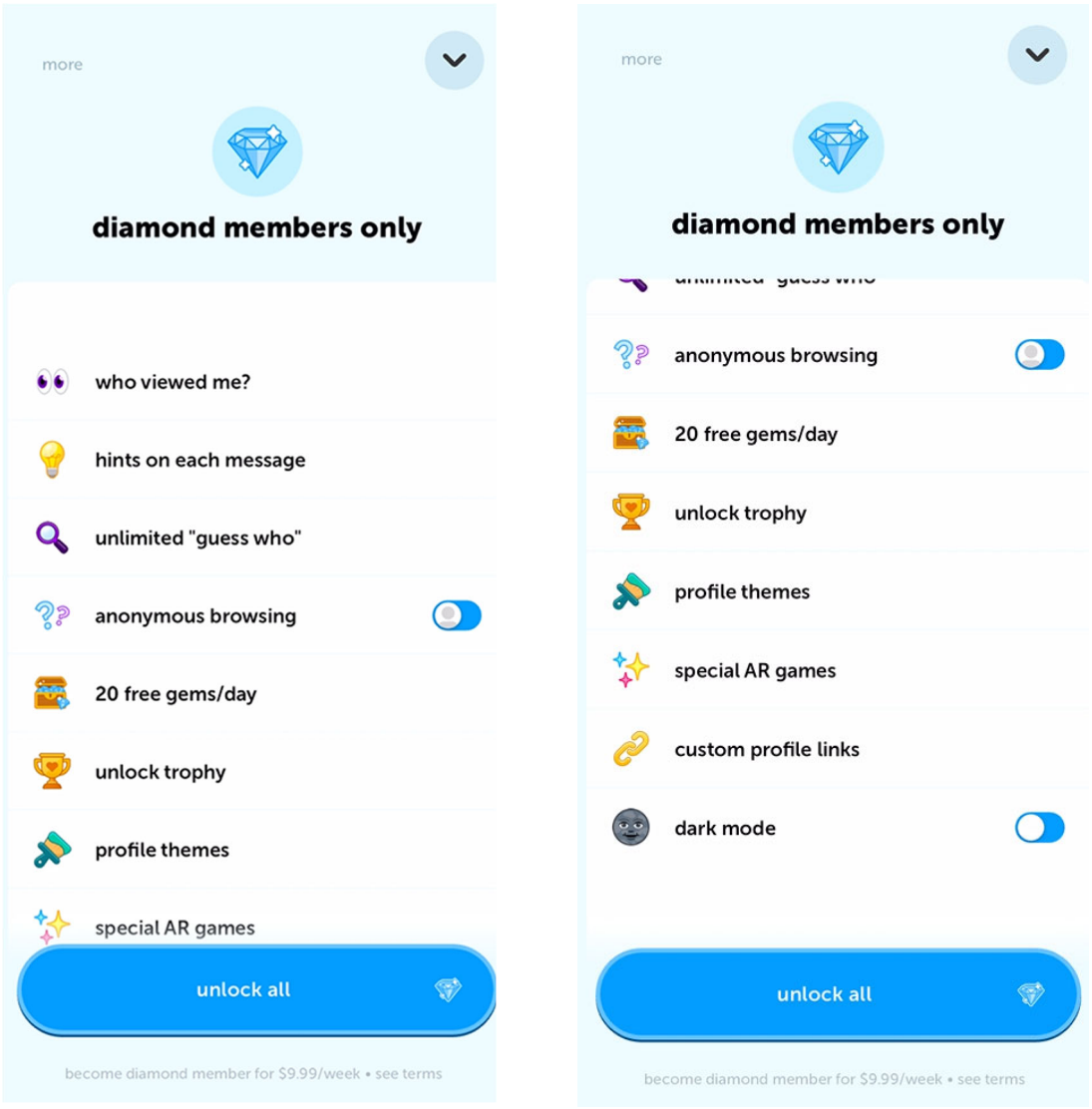
Image 5: First Call-to-Action Button in Diamond Membership Purchase in November 2023	Image 6: Second Call-to-Action Button in Diamond Membership Purchase in November 2023
	

24. Defendants also displayed other screens reinforcing the notion that a paid membership would reveal message senders' identities. For example, after clicking the large "see hint" button that is shown toward the bottom of Image 6, and still prior to making payment, consumers were directed to a page that describes

the features of the Diamond Membership (see, e.g., Image 7, listing "who viewed me," "hints on each message," and others). The screen had a prominent "unlock all" call-to-action button.

25. To the extent that Sendit's in-app screens enticing consumers to become Diamond Members to learn who sent them messages have disclosed at all that the membership was a recurring paid subscription, or how much that subscription costs, they have done so only in text that is inconspicuous due to its small size, lack of contrasting color, and non-prominent placement beneath call-to-action buttons. For example, a close inspection of Images 6 and 7 shows that, barely visible below the call-to-action buttons, in faint and miniscule font, was a vague disclosure that stated, "become diamond member for $9.99/week · see terms."

Image 7: Third Call-to-Action Button in Diamond Membership Purchase in November 2023



26. In or around June 2024, after learning of an FTC investigation into Sendit, Defendants made minor modifications to the language in the Diamond Membership call-to-action buttons. Despite the changes, Defendants continued to include only a vague disclosure, in light gray miniscule font, placed below the call-to action button. For example, Images 8, 9, and 10 (below) show Sendit's Diamond Membership in-app purchase flow that a consumer saw when reviewing a (fake or

real) anonymous message from June 2024, including a tiny line below the call-to-action buttons at the bottom of Images 9 and 10 reading "become diamond member for $8.99/week · view terms":

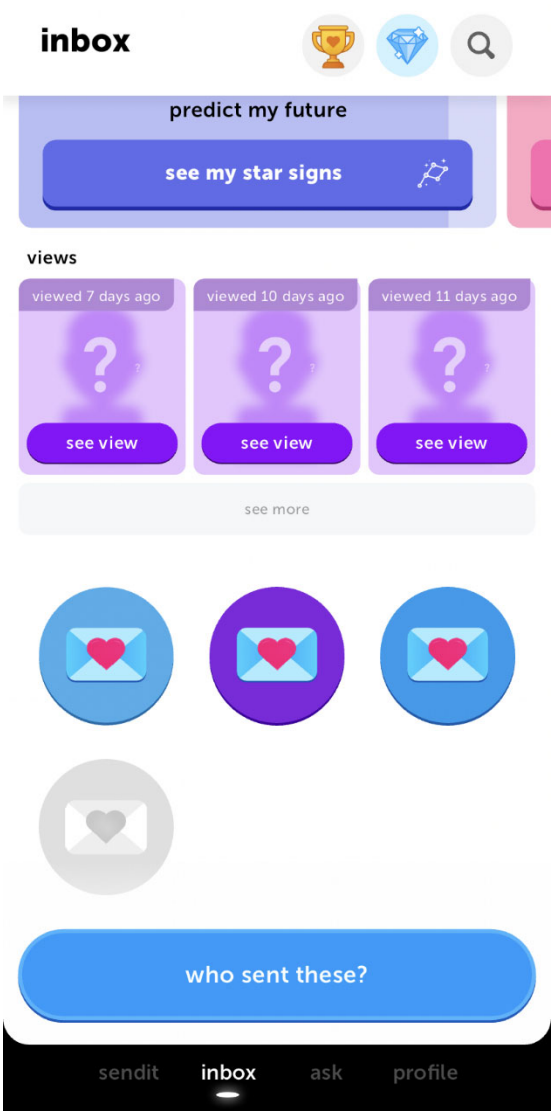
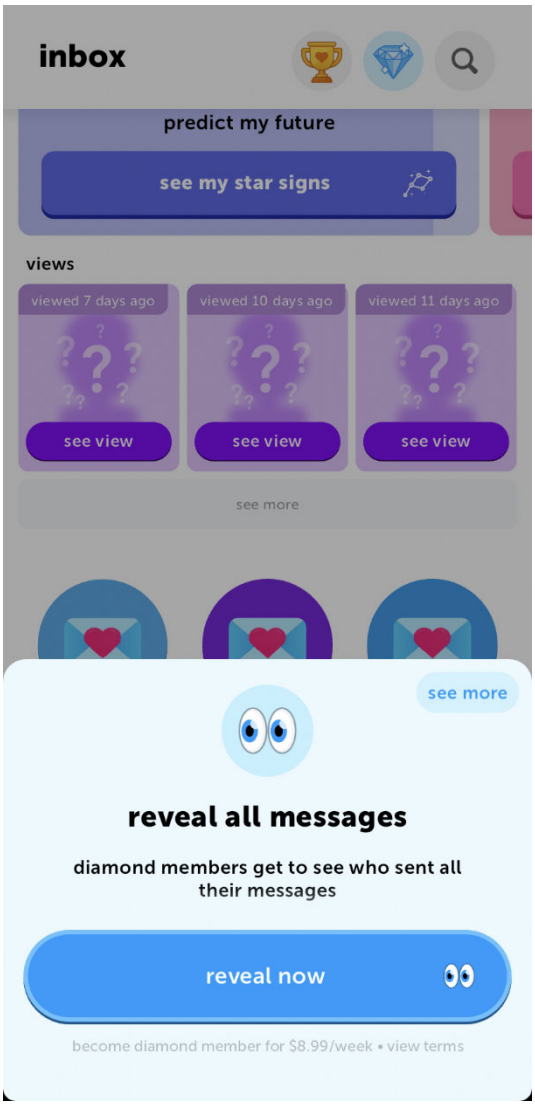
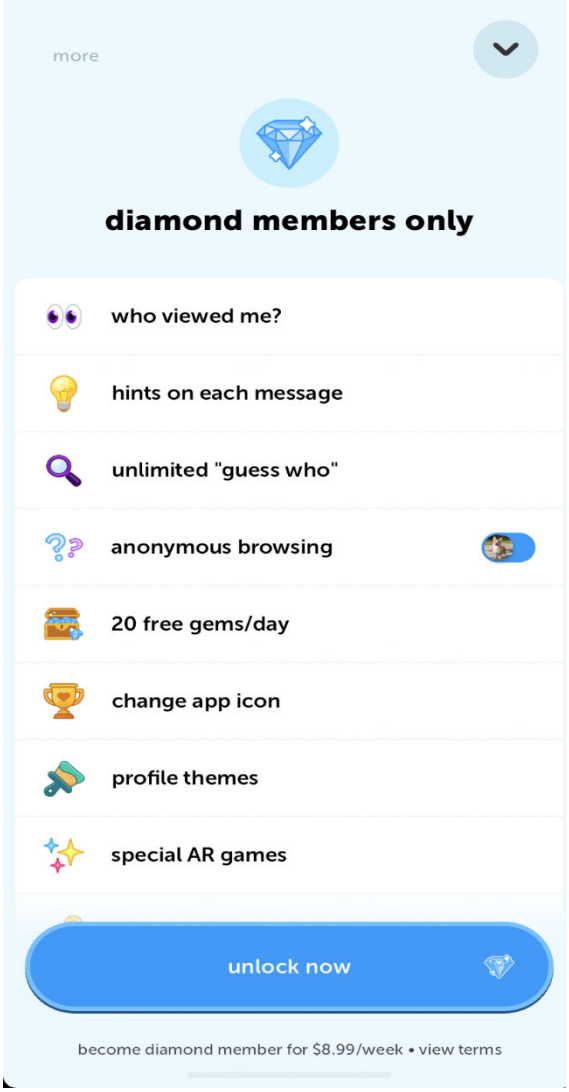
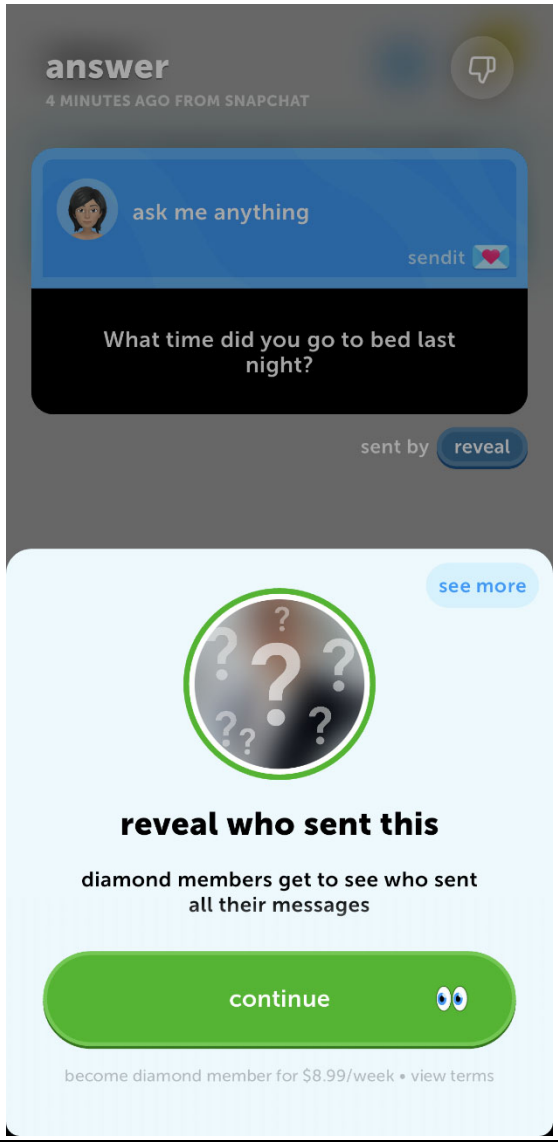
Image 8: First Call-to-Action Button in Diamond Membership Purchase in June 2024	Image 9: Second Call-to-Action Button in Diamond Membership Purchase in June 2024
	

Image 10: Third Call-to-Action Button in Diamond Membership Purchase in June 2024



27. Since they began offering the Diamond Membership, Defendants have experimented with some of the language in their call-to-action buttons that encourage users to purchase the Diamond Membership, but the essential offering has remained the same: users reviewing their anonymous messages see a prominent button below their messages offering the opportunity to find out "who sent" the message, at which point they click one to a few more buttons on Sendit to

enroll in the Diamond Membership. For example, below are screens that a user sees on a Sendit message as of June 2025, before purchasing the Diamond Membership:

Image 11: First Call-to-Action Button in Diamond Membership Purchase in June 2025	Image 12: Second Call-to-Action Button in Diamond Membership Purchase in June 2025
	

Defendants Use Fake Messages to Drive Users' Engagement With the App & Purchases of the Diamond Membership

28. From approximately early 2021 to at least late 2024, Defendants sought to increase users' engagement with Sendit and paid subscriptions to Sendit by sending fake messages—designed to look like real responses from users' actual social media contacts—in response to Sendit prompts. Defendants internally referred to these fake messages as "engagement posts." Below in Images 13–15 are examples of fake messages, which a Sendit user received after sharing a Sendit prompt privately on social media in such a manner that no real social media contacts or real people of any kind saw the post:

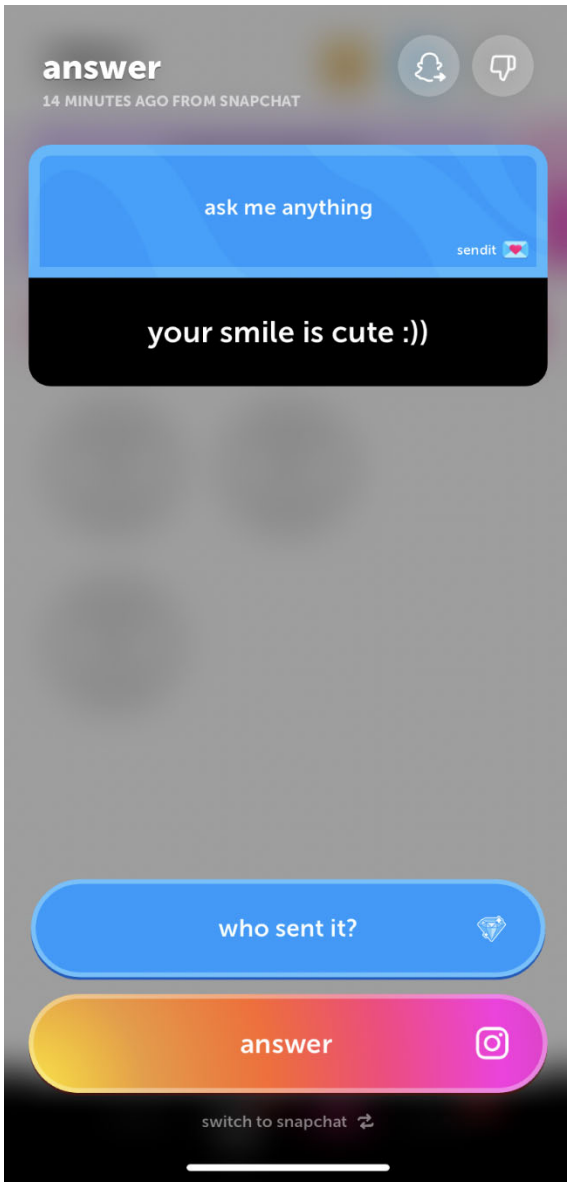
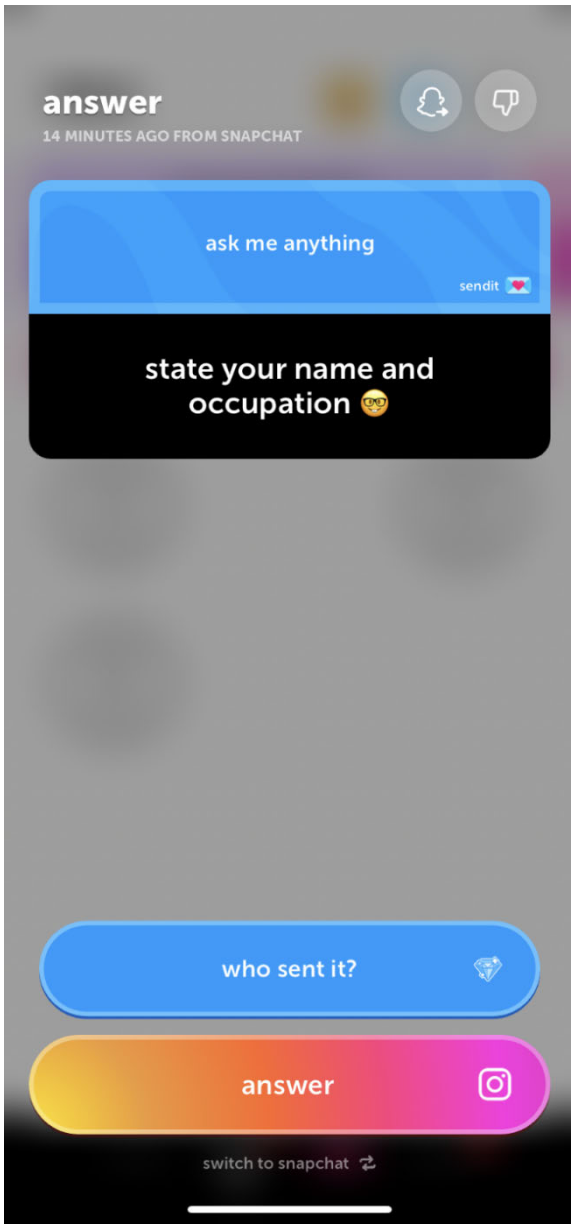
Image 13: Fake Message Captured in November 2023	Image 14: Fake Message Captured in November 2023
	

Image 15: Fake Message Captured in November 2023



29. As illustrated by the examples in Images 13–15 above, Defendants' fake messages gave the impression that Sendit users' real social media contacts were responding to the Sendit prompts that those users posted on their social media accounts. There is no way to tell from the messages alone that they are not real.

30. In fact, Defendants' fake messages, which were collectively sent approximately 279 million or more times to Sendit users, were chosen and sent by Defendants, taken from an inventory of more than 175 fake messages. This inventory included provocative statements and questions like:

- "have you done drugs"
- "I like you guess who it is"
- "Does size matter"
- "I know what you did"
- "take me on a date papi"
- "what the freakiest thing you did"
- "Have you ever passionately fantasized about me"
- "Do you like any body"
- "did you get with him or not"
- "what's your straight/bi ratio?"
- "You better see me when I come back home"
- "would you ever get with me?"
- "would you ever be f[riends] w[ith] b[enefits]"
- "whos ur crush?"
- "do you have trust issues?"
- "spill some tea"
- "any tips for fake friends who talk about and even whisper gossip about u literally next to u?"

Until around late 2024, the fake messages drawn from this list were sent to users without being labeled in any way to disclose that it was Iconic Hearts, rather than one of the consumers' social media contacts, who wrote and sent the fake message.

31. Many of Defendants' fake messages, including those listed in Paragraph 30, were provocative and manipulative, particularly when sent to children and teens. Some of these messages were adult-themed messages, while

others were flirtatious (such as, "I like you guess who it is," and "i love uuuuuu!!," and "Would it be crazy if I missed you like more then I thought I would") and misleadingly conveyed that someone was interested in the user. Others foreseeably created fear or anxiety among children and teens about private information their social media contacts might know or reveal (such as, "I know what you did" and "did you get with him or not").

32. Defendants profited from child and teen consumers' vulnerability to "catfishing," the act of deceiving someone into an interaction or relationship through impersonation or the use of a fake identity online. With these fake anonymous messages, Defendants lured children and teens into purchasing Sendit's "Diamond Membership" subscription, which purports to provide the subscriber with the identity of the senders of anonymous messages. Indeed, as shown in example Images 13–15 above, Defendants consistently paired their fake messages with the "who sent it" Diamond Membership offer at the bottom of the messages, to encourage the consumers to buy the Diamond Membership to find out who sent the fake message.

33. Many consumers complained that they were tricked into purchasing the Diamond Membership because of these fake messages. Many of the children and teens who later realized the provocative messages were fake felt manipulated by Sendit, and described the practice as "deceptive," "cruel," "hurtful," and "creepy."

34. Children, teens, and parents (whose payment cards were charged) were not able to reasonably avoid this substantial financial injury because they were unaware the messages were fake. This substantial injury was not outweighed by countervailing benefits to consumers or competition. Indeed, Defendants' practice of using fake messages to lure consumers into subscriptions has no benefit to consumers or competition.

35. In addition to increasing consumers' engagement with the Sendit app, Defendants' transmission of fake messages also led more Sendit consumers to purchase Diamond Membership subscriptions to find out "who sent" the fake messages, based on the false belief that these messages were from their real social media contacts.

The Diamond Membership Does Not Reveal the Identity of the Sender or Distinguish Between Fake and Real Messages

36. As described above, Defendants represented to consumers that Diamond Members would learn who sent them anonymous messages and obtain hints about those senders' identities. Moreover, Sendit's in-app advertising at times has made further representations to consumers about what information Diamond Members would learn, including for example that: (a) hints provided to Diamond Members would contain identifying information such as the "first initial of [the sender's] name, hair color, eye color, mutual friends, and other ways to find out who the person is"; and (b) consumers with a Diamond Membership "can reveal the [sender's] username and bitmoji."

37. Many consumers purchased the Diamond Membership because Defendants' advertising led them to believe that it would allow them to see the anonymous message sender's display name or to otherwise obtain information that would reveal the anonymous message sender's identity. Moreover, given that Sendit can obtain information about the anonymous message senders' identities from their social media accounts, consumers reasonably anticipated that "hints" would contain such information.

38. In reality, until at least June 2024, the Diamond Membership did not provide users with hints that helped reveal the identity of the senders of their anonymous messages. When consumers clicked on the "who sent it" button seeking hints about who sent the fake anonymous messages, the Diamond

Membership provided completely fabricated information.[1] Even for the real anonymous messages, the Diamond Membership's hints were functionally useless because they were limited to generic information such as: (a) the type of device an anonymous consumer is using (e.g., "Android" or "iPhone"); (b) the general location the sender was in at the time the message was sent (e.g., "Los Angeles"); or (c) general information about the sender's friend network on social media (e.g., "this user is friends with X"). Moreover, the hints did not offer additional information such as the "first initial of [the sender's] name, hair color, eye color, mutual friends," despite Defendants' representations to the contrary.

39. Instead, Defendants would reveal a message sender's display name to the Diamond Membership purchaser only if they made an additional one-time "Reveal" in-app purchase, for which Defendants generally charged the consumer an additional $29.99. The option to make this "Reveal" purchase would often be prominently offered to consumers only after they purchased the Diamond Membership and received a useless "hint."

40. Defendants generated tens of millions of dollars in revenue from Diamond Membership purchasers who were falsely promised that they would receive information identifying the senders of their anonymous messages.

41. Many consumers who purchased the Diamond Membership complained to Iconic Hearts seeking refunds and left negative reviews in the Apple App Store and Google Play Store.

42. Consumers' dissatisfaction with the Diamond Membership generated so many refund requests and complaints that in February 2022, Apple threatened to remove Sendit from its app store for violating Apple's Developer Code of

[1] For example, upon purchasing the Diamond Membership to find out "who sent" the fake messages in Images 13–15, the Sendit user and Diamond Membership purchaser received the same hints for all three messages: "hint: they are located in long beach and have an iphone."

Conduct. In response, Rice falsely represented to Apple that Defendants would make the Diamond Membership more valuable by adding more specific hints and by ensuring that all messages are sent by real humans.

43. Despite these representations to Apple, Sendit did not offer more specific hints to users for at least two more years, until after the FTC began an investigation of Sendit. Nor did the Defendants ensure that all messages are sent by real humans.

Defendants Fail to Clearly and Conspicuously Disclose and Obtain Informed Consent for Recurring Diamond Membership Charges

44. In addition to misrepresenting the benefits of the Diamond Membership, Defendants have also continuously failed to clearly and conspicuously disclose that the Diamond Membership is an automatically renewing subscription for which the consumer will be charged every week unless they take affirmative action to cancel it.

45. Defendants led consumers through a series of screens with call-to-action buttons enticing consumers to become Diamond Members prior to the consumer's purchase of an automatically renewing subscription. For example, in the pre-June 2024 version of a user flow depicted in Images 5-7 above, clicking the "who sent it" button leads to a "see hint" button, and then a final "unlock all" button. In the June 2024 version of a user flow depicted at Images 8-10 above, clicking the "who sent these" button leads to a "reveal all messages" button, and then a final "unlock all" button. In the June 2025 version of a user flow depicted at Images 11-12 above, clicking the "reveal who sent this" button leads to a final "continue" button before purchase.

46. Throughout the various iterations of the Diamond Membership purchase flow, Defendants have continuously failed to clearly or conspicuously disclose to consumers following material terms of the transaction, including: (a) the purchase price (e.g., $9.99 or $8.99 per week); (b) the facts that the purchase

price will be automatically charged on a recurring basis, weekly, unless affirmatively cancelled. The purported disclosures are vaguely worded (e.g., "become diamond member for $9.99/week · see terms" or "become diamond member for $8.99/week · view terms") and presented in an inconspicuous manner, such as in a barely visible, miniscule light gray font set against a non-contrasting background, placed below the call-to-action buttons.

47. Many consumers have complained that because of Defendants' inadequate disclosures, they were tricked into buying a subscription, when they intended to make at most only a single purchase to find out "who sent" an individual anonymous message in their Sendit inbox.

48. Despite Defendants' inadequate disclosures and the complaints and refund requests they received from numerous subscribers, Defendants rarely, if ever, provided refunds for Diamond Membership subscriptions.

49. Defendants have actual knowledge or knowledge fairly implied on the basis of objective circumstances, including through their written policies and agreements with third parties, that their actions are deceptive and prohibited by ROSCA.

***

50. The FTC informed Defendants in July 2023 that Iconic Hearts was being investigated for potential violations of ROSCA, COPPA, the COPPA Rule and Section 5 of the FTC Act. Nevertheless, Defendants' unlawful conduct continued.

51. Based on the facts and violations of law alleged in this Complaint, Plaintiff has reason to believe that Defendants are violating or are about to violate the COPPA Rule, the FTC Act, and ROSCA.

VIOLATIONS OF THE COPPA RULE

52. Congress enacted COPPA in 1998 to protect the safety and privacy of children online by prohibiting the unauthorized or unnecessary collection of

children's personal information online by operators of Internet websites and online services. COPPA directed the FTC to promulgate a rule implementing COPPA. The FTC promulgated the COPPA Rule, 16 C.F.R. Part 312, on November 3, 1999, under Section 1303(b) of COPPA, 15 U.S.C. § 6502(b), and Section 553 of the Administrative Procedure Act, 5 U.S.C. § 553. The Rule went into effect on April 21, 2000. The FTC promulgated revisions to the Rule that went into effect on July 1, 2013.

53. The Rule applies to any operator of a commercial website or online service directed to children under 13 years of age (which includes operators of online services with actual knowledge that they are collecting personal information directly from users of another website or online service directed to children), or any operator that has actual knowledge that it is collecting or maintaining personal information from a child under 13 years of age. 16 C.F.R. § 312.3. The definition of "personal information" includes, among other things, a "first and last name," "online contact information," "a screen name or user name," a "persistent identifier that can be used to recognize a user over time and across different Web sites or online services," such as a "customer number held in a cookie, an Internet Protocol (IP) address, a processor or device serial number, or unique device identifier," a "photograph, video, or audio file where such file contains a child's image or voice," and "[i]nformation concerning the child or the parents of that child that the operator collects online from the child and combines with an identifier described in this definition." 16 C.F.R. § 312.2.

54. Among other things, the Rule requires subject operators to meet specific requirements related to collecting, using, or disclosing personal information from children, which includes

- Providing clear, understandable, and complete notice of its information practices, including specific disclosures, directly to parents, including what information the operator collects from

children online, how it uses such information, its disclosure practices for such information, and other specific disclosures set forth in the Rule; and

- Obtaining verifiable parental consent prior to collecting, using, and/or disclosing children's personal information.

55. Pursuant to Section 1303(c) of COPPA, 15 U.S.C. § 6502(c), and Section 18(d)(3) of the FTC Act, 15 U.S.C. § 57a(d)(3), a violation of the Rule constitutes an unfair or deceptive act or practice in or affecting commerce, in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

COUNT I

Violation of the COPPA Rule

56. Paragraphs 1 through 55 are incorporated as if set forth herein.

57. Defendants are "operators" subject to the COPPA Rule.

58. Defendants collect personal information from children through the Sendit app, which is an online service or website directed to children. Defendants have actual knowledge that they are collecting personal information from children through the Sendit app.

59. In connection with the acts and practices described above, Defendants have collected and used personal information from children in violation of the Rule, including by:

a) failing to make reasonable efforts to provide direct notice to parents of the information Defendants collect from children through their website or online service, how they use such information, and their disclosure practices for such information, among other required content, in violation of 16 C.F.R. § 312.4(b)–(c);

b) failing to obtain consent from parents before any collection or use of personal information from children, while

i. failing to limit their collection of children's personal information for which they lacked verifiable parental consent to only the limited information permitted by the Rule's exceptions to prior parental consent requirements, and

ii. failing to limit their collection and use of children's personal information for which they lacked verifiable parental consent to solely the purposes permitted by the Rule (such as the use of a persistent identifier for the sole purpose of providing support for the internal operations of their website or online service),

in violation of 16 C.F.R. § 312.5.

60. Defendants committed these violations with the knowledge required by Section 5(m)(1)(A) of the FTC Act, 15 U.S.C. § 45(m)(1)(A).

61. Each collection, use, or disclosure of a child's personal information in which Defendants violated the Rule in one or more of the ways described above constitutes a separate violation for which Plaintiff seeks monetary civil penalties.

62. Each day Defendants maintained data collected in violation of the Rule, or otherwise continued to collect such data, is a continuing failure to comply with the Rule and constitutes a separate violation under 15 U.S.C. § 45(m)(1)(C).

63. Section 5(m)(1)(A) of the FTC Act, 15 U.S.C. § 45(m)(1)(A), as modified by Section 4 of the Federal Civil Penalties Inflation Adjustment Act of 1990 and Section 701 of the Federal Civil Penalties Inflation Adjustment Act Improvements Act of 2015, 28 U.S.C. § 2461, and Section 1.98(d) of the FTC's Rules of Practice, 16 C.F.R. § 1.98(d), authorizes this Court to award monetary civil penalties of not more than $53,088 for each violation of the Rule assessed after January 17, 2025.

VIOLATIONS OF THE FTC ACT

64. Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), prohibits "unfair or deceptive acts or practices in or affecting commerce."

65. Misrepresentations or deceptive omissions of material fact constitute deceptive acts or practices prohibited by Section 5(a) of the FTC Act.

66. Acts or practices are unfair under Section 5 of the FTC Act if they cause or are likely to cause substantial injury to consumers that consumers cannot reasonably avoid themselves and that is not outweighed by countervailing benefits to consumers or competition. 15 U.S.C. § 45(n).

COUNT II

Misrepresentations Regarding Sendit and the Diamond Membership

67. Paragraphs 1 through 66 are incorporated as if set forth herein.

68. In connection with the advertising, marketing, promoting, and offering for sale of Sendit and of services to Sendit users, Defendants have misrepresented, directly or indirectly, expressly or by implication:

a) the nature and origin of messages that a consumer using Sendit receives; and

b) the characteristics, benefits, and costs of the services Defendants sell consumers.

69. Defendants' representations constitute deceptive acts or practices in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

COUNT III

Unfair Use of Fake Messages to Market Sendit and the Diamond Membership to Child and Teen Users

70. Paragraphs 1 through 69 are incorporated as if set forth herein.

71. Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), prohibits "unfair or deceptive acts or practices in or affecting commerce."

72. Acts or practices are unfair under Section 5 of the FTC Act if they cause or are likely to cause substantial injury to consumers that consumers cannot reasonably avoid themselves and that is not outweighed by countervailing benefits to consumers or competition. 15 U.S.C. § 45(n).

73. In numerous instances, in connection with the advertising, marketing, promoting, and offering for sale of Sendit and the Diamond Membership, the Defendants, in the context of an anonymous message platform, have composed and sent child and teen users messages, sometimes of a provocative, romantic, or sexual nature, for the purpose of tricking child and teen users into the purchase of subscriptions to reveal the identity of the sender.

74. Defendants' acts or practices have caused or were likely to cause substantial injury to consumers that consumers cannot reasonably avoid themselves and that is not outweighed by countervailing benefits to consumers or competition.

75. Therefore, Defendants' acts or practices constituted unfair acts or practices in violation of Section 5 of the FTC Act, 15 U.S.C. § 45(a), (n).

VIOLATIONS OF THE RESTORE ONLINE SHOPPERS' CONFIDENCE ACT

76. The Restore Online Shoppers' Confidence Act, 15 U.S.C. §§ 8401-05, became effective on December 29, 2010. Congress passed ROSCA recognizing that: "[c]onsumer confidence is essential to the growth of online commerce. To continue its development as a marketplace, the Internet must provide consumers with clear, accurate information and give sellers an opportunity to fairly compete with one another for consumers' business." Section 2 of ROSCA, 15 U.S.C. § 8401.

77. ROSCA prohibits certain unfair or deceptive practices for internet sales with a "negative option feature," which is defined as: "in an offer or agreement to sell or provide any goods or services, a provision under which the consumer's silence or failure to take an affirmative action to reject goods or

services or to cancel the agreement is interpreted by the seller as acceptance of the offer" by the Telemarketing Sales Rule ("TSR"),16 C.F.R. § 310.2(w).

78. ROSCA generally prohibits charging consumers for a good or service sold in a transaction effected on the Internet through a negative option feature, unless the seller, among other things: (1) clearly and conspicuously discloses all material terms of the transaction before obtaining the consumer's billing information and (2) obtains the consumer's express informed consent before making the charge. 15 U.S.C. § 8403.

79. Pursuant to Section 5 of ROSCA, 15 U.S.C. § 8404, and Section 18(d)(3) of the FTC Act, 15 U.S.C. § 57a (d)(3), a violation of ROSCA constitutes an unfair or deceptive act or practice in or affecting commerce in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

COUNT IV

Violations of ROSCA – Inadequate Disclosures & Failure to Obtain Express Informed Consent

80. Paragraphs 1 through 79 are incorporated as if set forth herein.

81. In connection with charging consumers for a good or service sold in a transaction effected on the Internet through a negative option feature, Defendants have failed to:

a) clearly and conspicuously disclose all material terms of the transaction before obtaining the consumer's billing information; and

b) obtain the consumer's express informed consent before charging the consumer's credit card, debit card, bank account, or other financial account through such transaction.

82. Therefore, Defendants' acts or practices violate Section 4 of ROSCA, 15 U.S.C. § 8403, and Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

83. Defendants committed these violations with the knowledge required by Section 5(m)(1)(A) of the FTC Act, 15 U.S.C. § 45(m)(1)(A).

CONSUMER INJURY

84. Consumers are suffering, have suffered, and will continue to suffer substantial injury as a result of Defendants' violations of the COPPA Rule, the FTC Act, and ROSCA. Absent injunctive relief by this Court, Defendants are likely to continue to injure consumers and harm the public interest.

CIVIL PENALTIES

85. Section 5(m)(1)(A) of the FTC Act authorizes this Court to award monetary civil penalties for each violation of the COPPA Rule and ROSCA.

86. Defendants violated the COPPA Rule and ROSCA with the knowledge required by Section 5(m)(1)(A) of the FTC Act, 15 U.S.C. § 45(m)(1)(A).

PRAYER FOR RELIEF

Wherefore, Plaintiff requests that the Court:

A. Enter a permanent injunction to prevent future violations of the COPPA Rule, the FTC Act, and ROSCA;

B. Award monetary and other relief within the Court's power to grant;

C. Impose civil penalties on each Defendant for every violation of the COPPA Rule and ROSCA; and

D. Award any additional relief as the Court determines to be just and proper.

Dated: September 29, 2025

Respectfully submitted,

OF COUNSEL, FOR THE FEDERAL TRADE COMMISSION:

SIOBHAN C. AMIN
MILES D. FREEMAN
JOHN D. JACOBS
Federal Trade Commission
10990 Wilshire Boulevard, Suite 400
Los Angeles, CA 90024
Tel: (310) 824-4300
samin@ftc.gov

FOR THE UNITED STATES OF AMERICA:

BRETT A. SHUMATE
Assistant Attorney General, Civil Division

JORDAN C. CAMPBELL
Deputy Assistant Attorney General

SARMAD M. KHOJASTEH
Senior Counsel

LISA K. HSIAO
Acting Director, Consumer Protection Branch

ZACHARY A. DIETERT
Assistant Director

/s/ Marcus P. Smith
MARCUS P. SMITH
Trial Attorney
Consumer Protection Branch
Civil Division, U.S. Department of Justice
450 5th Street, NW, Suite 6400-South
Washington, DC 20001
Tel.: (202) 353-9712
Fax: (202) 514-8742
Email: Marcus.P.Smith@usdoj.gov