162-3102

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: **Joseph J. Simons, Chairman**
Maureen K. Ohlhausen
Noah Joshua Phillips
Rohit Chopra
Rebecca Kelly Slaughter

In the Matter of **PAYPAL, INC., a corporation.**	**DOCKET NO. C-4651**

COMPLAINT

The Federal Trade Commission, having reason to believe that PayPal, Inc., a corporation, ("Respondent") has violated Section 5(a) of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45(a); the Privacy of Consumer Financial Information ("Privacy Rule"), 16 C.F.R. Part 313, recodified at 12 C.F.R. Part 1016 ("Reg. P"), and issued pursuant to the Gramm-Leach-Bliley Act ("GLB Act"), 15 U.S.C. §§ 6801-6803; and the Standards for Safeguarding Customer Information Rule ("Safeguards Rule"), 16 C.F.R. Part 314, issued pursuant to Sections 501(b) and 505(b)(2) of the GLB Act, 15 U.S.C. §§ 6801(b), 6805(b)(2); and it appearing to the Commission that this proceeding is in the public interest, alleges:

1. Respondent PayPal, Inc. is a Delaware corporation with its principal place of business at 2211 North First Street, San Jose, California 95131.

2. Respondent operates Venmo, a payment and social networking application and website that allows consumers to make peer-to-peer payments and to share information regarding such payments through a social network feed.

3. The acts and practices of Respondent alleged in this complaint have been in or affecting commerce, as "commerce" is defined in Section 4 of the FTC Act.

VENMO'S BUSINESS PRACTICES

Background on the Venmo Peer-to-Peer Payment System

4. Venmo has offered its peer-to-peer payment service to consumers since 2011. The service was previously provided by a Delaware corporation of the same name, and, since an acquisition in 2013, has been provided by Respondent operating as Venmo.

5. Consumers can download the Venmo application (the "app") onto their mobile devices and use Venmo through its website, Venmo.com. Consumers create a Venmo account to which they may connect external bank accounts, debit cards, or credit cards. The Venmo account can receive money—creating a Venmo "balance"—from other Venmo users or from linked external sources. Consumers can send money from their Venmo balance to other Venmo users, and, if they do not have enough money in their Venmo balance to cover a transaction, the funds are drawn from their attached external account. Consumers can also transfer money from their Venmo balance to their external bank accounts.

6. To initiate a Venmo transaction, a Venmo user may either send money to another Venmo user or submit a "charge request" that asks the recipient to pay money to the requesting user. Users must also include a short message that accompanies each transaction.

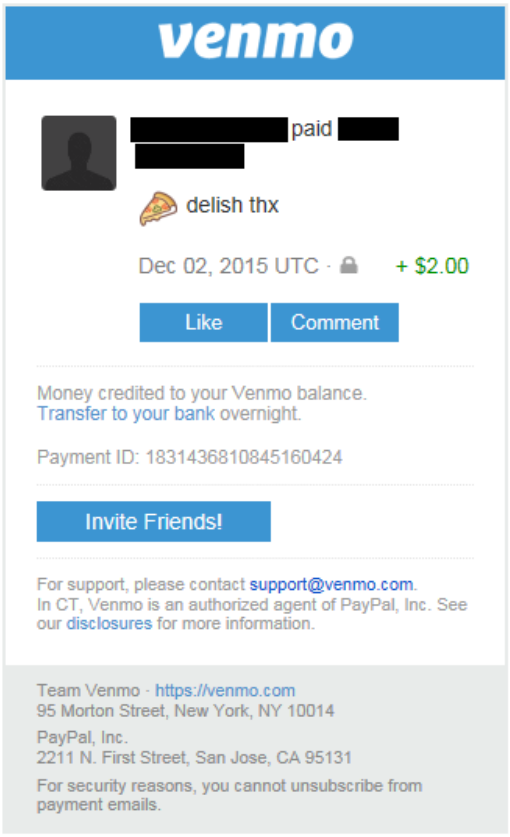
7. As described further below, by default, Venmo publicly shares the names of the participants of a transaction, the date of the transaction, and any accompanying message regarding the transaction on a social news feed on the Venmo service.

8. As Venmo explains prominently on its website and in mobile application stores, consumers can use the service for a variety of purposes including to "make purchases" and that they can use the service "with anyone." For example, at various times, the "How it works" page of the Venmo website has stated that consumers can "Use Venmo with anyone," "Pay anyone with a Venmo account instantly," and "Pay family and friends … ." Venmo also has noted that "anyone" includes individuals who are not yet Venmo users.

9. Venmo's public social network feed is visible on its homepage and has shown consumers conducting transactions such as "tickets," "baby watching," "lunch," "bills," "rent," "taxi," and "iphone repair."

Venmo's Representations About Money Transfers

10. When a Venmo user sends money through Venmo to another user, the recipient receives a notification within seconds of the sender initiating the transfer. These notifications appear within the Venmo app, and consumers can additionally choose to receive these notifications via text message, email, or "push notifications" that appear on the screen of the consumer's mobile device. In numerous instances, the notifications have informed the recipients that they have been paid and they can transfer money to their external bank accounts. For example, at various times, the notifications have read "Money credited to your Venmo balance. Transfer to your bank overnight." Other notifications have told consumers that someone "paid $[X] to your Venmo balance [description of transaction.] -- Leave it in Venmo or transfer it to your bank account." An example of an email notification that Venmo has used appears as follows:



11. In addition to these transaction-specific representations, Venmo has represented generally that consumers can transfer funds to their bank within a specific time frame, often "overnight." For example, at various times Venmo's homepage has stated that consumers who were sent funds through the Venmo system could "cash out to any bank overnight." Venmo has used a similar description in the Google Play store website, which stated "Transfer money to any bank overnight," and the Google Play store on consumers' mobile devices stated "Cash out to any bank overnight." Similarly, the Venmo description on the Apple store for mobile devices and on the Apple store on consumers' personal computers has stated "Transfer to any bank overnight." More recently, Respondent's "How It Works" page has stated "Quickly transfer money to your bank" and "Move money from Venmo to your bank account in as little as one business day."

12. As a result of these representations, many consumers believe that, when they receive payment notifications from Venmo, the funds are ready to be transferred to an external bank account.

Problems Transferring Funds Out of Venmo

13. Despite these claims, in numerous instances, consumers have been unable to transfer funds to their bank accounts as promised. Venmo has waited until a consumer attempts to transfer funds to his or her external bank account to review the transaction for fraud,

insufficient funds, or other problems. This review has resulted in Venmo delaying the transfer or reversing the transaction, including in circumstances that the sender is a new user (notwithstanding Venmo's representations that consumers can use Venmo with "anyone"), that the consumer has engaged in a "business transaction" (notwithstanding Venmo's representations that consumers can use Venmo for "purchases"), or that the transaction has involved an amount of money above a certain threshold. In numerous instances, Venmo has required consumers to provide documentation or other information as part of its review. In numerous instances, Venmo has frozen consumers' accounts during the review. When Venmo reverses a transaction, it removes the funds from that transaction from the consumer's Venmo balance.

14. Despite its claims that money has been credited and can be transferred to consumers' external bank accounts, Venmo has not verified or approved consumer transactions until after consumers have initiated a transfer of funds to an external account, which could result in either substantial delays in the transfer or the reversal of the transaction. Venmo has failed to disclose this fact.

Venmo Was Aware of Consumer Confusion

15. Many thousands of consumers have complained to Venmo about the delays or loss of funds from their Venmo balance when they tried to transfer funds to their bank accounts. News articles from several media outlets since at least 2015 have highlighted the harm to consumers, which is sometimes in the thousands of dollars. Many consumers have reported suffering significant financial hardship due to not being able to transfer funds, including the inability to pay rent or bills with funds they expected to transfer out of Venmo. Other consumers have relied on the notifications indicating a sender paid them and supplied event tickets or other valuable items to the sender in exchange for funds, and consequently incurred a financial loss when Venmo removed the funds from their balance. In numerous instances, consumers who have attempted to contact Venmo have been unable to reach a representative or have not been provided with an explanation for or resolution to the problem with their account.

16. Internal company emails also have demonstrated that at least as early as mid-2015 Venmo was aware of "user frustration" and confusion experienced by consumers whose accounts were frozen or who suffered financial loss when transactions were reversed. Nevertheless, Venmo has continued representing, without qualification, that once money is credited to consumers' Venmo accounts, consumers can transfer the money to their bank accounts.

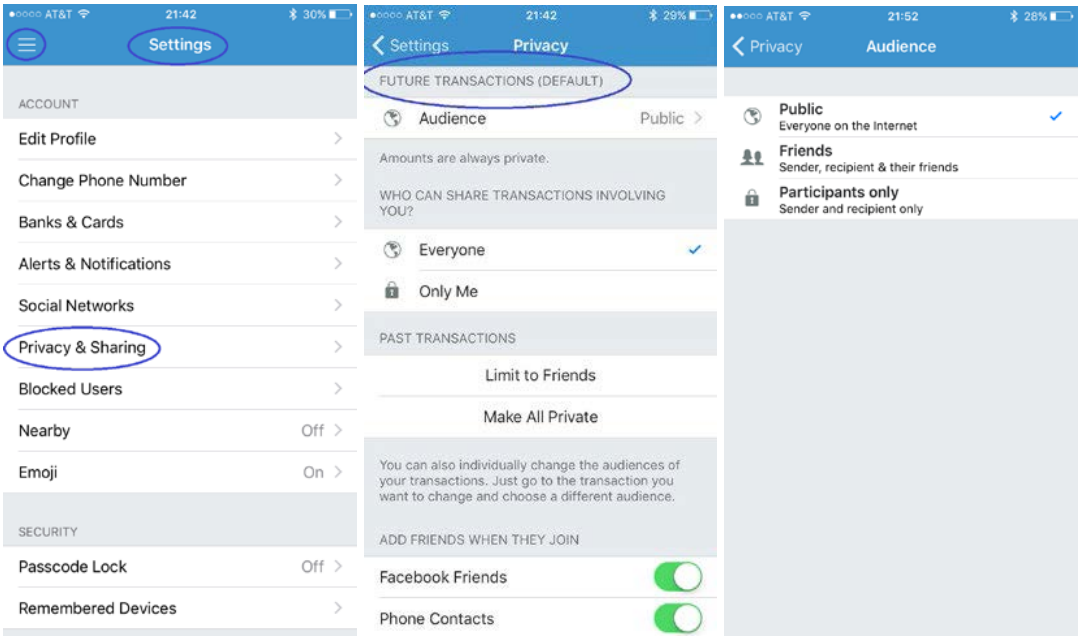
Venmo's Representations About Privacy

17. By default, all peer-to-peer transactions on Venmo are displayed on the Venmo social news feed. On this news feed, Respondent displays the names of the payer and recipient, the date of the transaction, and a message written by the user that initiated the transaction, to anyone using Respondent's service. In addition, each Venmo user has a profile page on Respondent's website that lists the user's Venmo transactions. A user's five most recent public Venmo transactions are visible, by default, to anyone who views the user's Venmo web page, including to visitors who do not have a Venmo account.

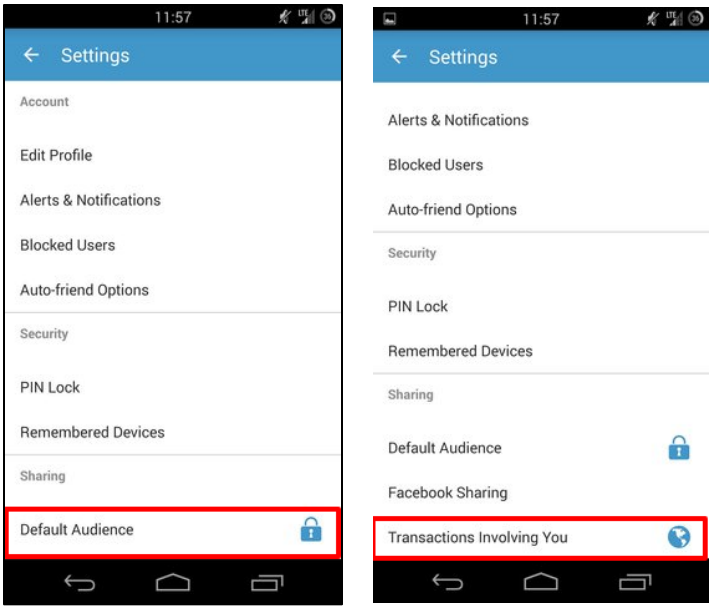
18. Consumers who do not want to share their Venmo transactions may restrict the visibility of their transactions through privacy settings available in a "Settings" menu or by configuring settings for an individual transaction.

19. Consumers who wish to generally restrict the visibility of all of their future transactions may do so through Venmo's "Settings" menu. To ensure that all payments remain private, a consumer must change two similarly labeled settings. The first setting in this menu limits the "default audience" for "future transactions" (hereinafter, the "Default Audience Setting"). A second setting, described in more detail below, controls "who can share transactions involving" the Venmo user (hereinafter, the "Transaction Sharing Setting"). Although these two settings appear on the same screen on both the iOS and the web-based version of the service, on some Android devices the Transaction Sharing Setting is only accessible if the user scrolls down below the Default Audience Setting.

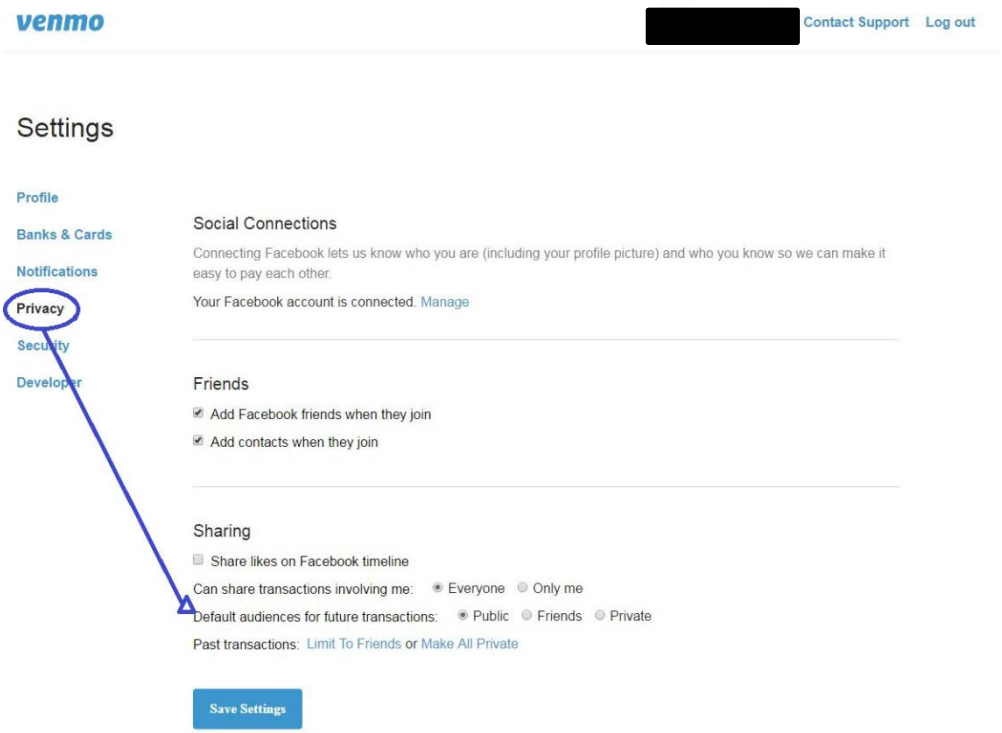
20. On Venmo's iOS app, privacy settings are accessible from a "Settings" menu, the same or similar to the one depicted below, from which a user may select "Privacy & Sharing." The Default Audience Setting is labeled "Future Transactions (Default)." The Transaction Sharing Setting is labeled "Who Can Share Transactions Involving You?"



21. On Venmo's Android App, the privacy settings menu appears the same or similar to the screenshots depicted below:



22. On the Venmo webpage, the privacy settings menu appears the same or similar to the screenshot depicted below:



23. The Default Audience Setting purports to allow the user to select the "audience" for all future transactions. It contains three options, identified as:

a) Public (Everyone on the Internet);

b) Friends (Sender, recipient & their friends); and

c) Participants only (Sender and recipient only).

24. The label describing the Default Audience Setting would lead a reasonable consumer to believe that she could limit the visibility of all of her future transactions by restricting this setting. Thus, a consumer who sets the Default Audience Setting to "Participants Only" would likely assume that, by default, all of her transactions will be viewable only by the participants of the transaction, regardless of whether she is the initiator or recipient of a transaction.

25. In fact, however, a consumer must also change Venmo's second setting, the Transaction Sharing Setting, in order to ensure that all of her transactions are private. As depicted in the screenshots above, the Transaction Sharing Setting contains two options: "Everyone" or "Only Me." By default, it is set to "Everyone." If a consumer fails to change the Transaction Sharing Setting to "Only Me," some of her transactions will still be published publicly even if she has chosen a "private" default audience through the Default Audience Setting.

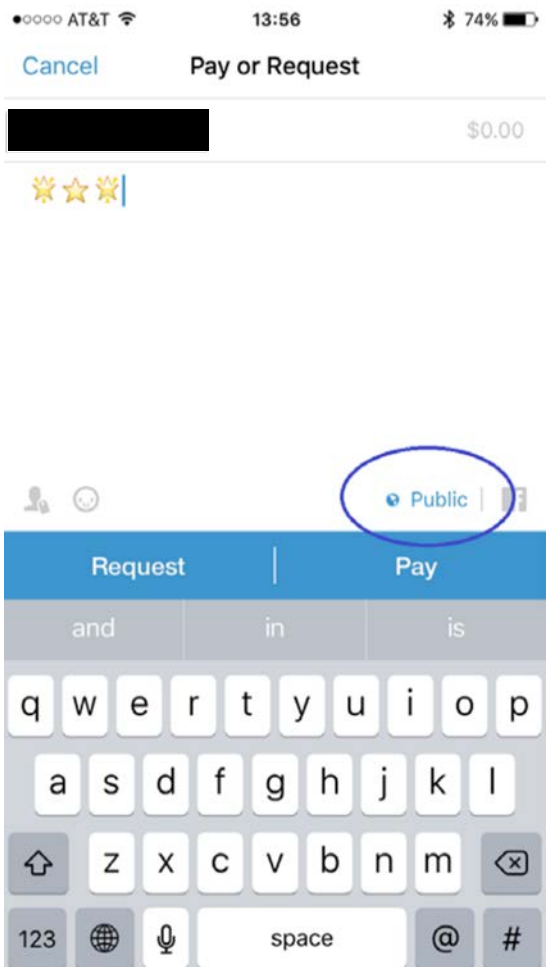
26. For example, suppose User A changes the Default Audience Setting to "Participants Only" but does not change the Transaction Sharing Setting to "Only Me." User B, meanwhile, leaves the Default Audience Setting set to "Public" and the Transaction Sharing Setting set to "Everyone." This configuration has the effect of overriding User A's clearly expressed privacy preferences in at least two ways:

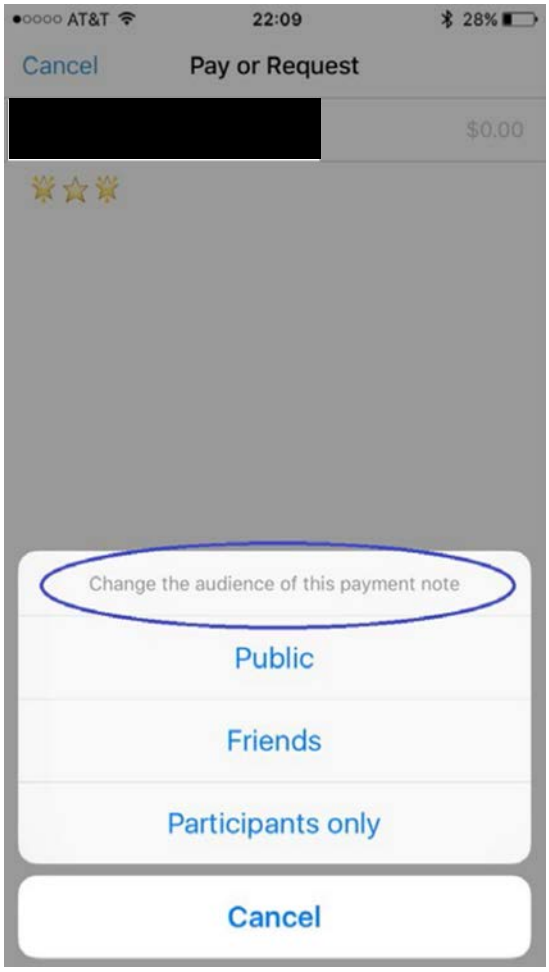
a) First, this configuration does not affect the privacy of any transactions where User A is the *recipient* of a transaction rather than the *initiator*. Thus, if User A sends a payment to User B, the transaction will be visible only to the participants, but if User B sends a payment or a charge request to User A, the transaction will be public and show User A as a recipient of User B's public transaction.

b) Second, even where User A initiates a private transaction, this configuration permits User B to retroactively make that transaction publicly viewable at any time after the transaction is complete, without providing any notice to User A.

27. Venmo has not informed consumers that the Transaction Sharing Setting permits another Venmo user to override the consumer's default audience or to retroactively make a private transaction public. These results are directly contrary to the expectations of a reasonable consumer.

28. Venmo also allows consumers to change the audience for individual transactions without engaging with the "Settings" menu. Thus, if a user only wants a particular transaction to be kept private, she could change the audience setting for an individual transaction at the time she sends a payment (hereinafter, the "Individual Audience Setting"). On Venmo's iOS app, the Individual Audience Setting appears the same or similar to the screenshot depicted below:





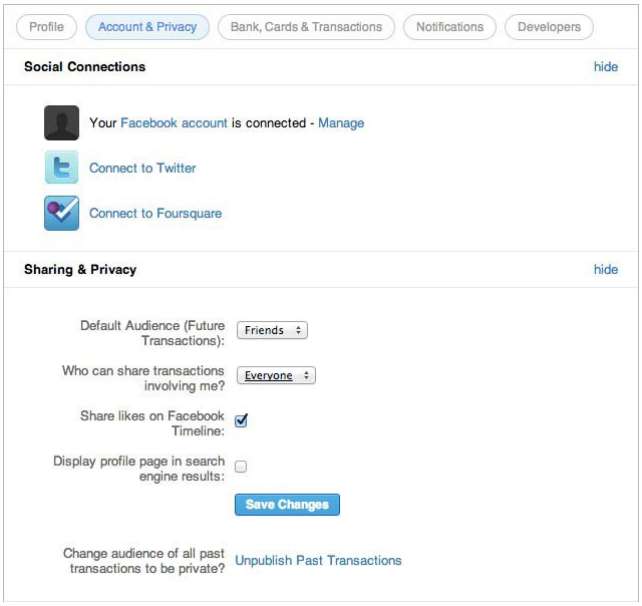
29. As with the Default Audience Setting, the Individual Audience Setting does not ensure that a transaction remains private unless a user has separately changed the Transaction Sharing Setting to "Only Me." If a user has not changed both settings, the other participant in the transaction may retroactively make the transaction public, as described in Paragraph 26(b).

30. Venmo has never informed consumers that the Transaction Sharing Setting permits retroactive changes to the visibility of a transaction, even where one participant has specifically intended for a transaction to be private. In fact, Venmo exacerbates these problems by incorrectly describing its privacy settings in its Privacy FAQs. For example, until at least December 2015, as depicted below, Venmo's Privacy FAQ included a graphic that incorrectly described the settings necessary to make a user's transactions private. Specifically, the graphic only restricts the Default Audience Setting while leaving the Transaction Sharing Setting unchanged.

FUTURE PAYMENTS

You can set up your Venmo account so that all future payments are private, to do so, follow these instructions:

- Log in to venmo.com (/web/20150525161659/https://venmo.com/)
- Navigate to **Account** -> **Account & Privacy** -> **Sharing & Privacy** -> **Edit**
- Choose your desired settings
- **Save**



31. In addition, in early 2017, Venmo revised this Privacy FAQ to state that "[s]etting your default audience to "Private" or "Participants Only" will ensure that your payments are only visible to you and the other participant in the payment." As described in paragraphs 25, 26 and 30, this statement is false.

Venmo's Representations About Security

32. Venmo has disseminated public statements on its mobile app and website about its information security practices, including the following:

a. "Venmo uses bank-grade security systems and data encryption to protect your financial information."

b. "Venmo uses bank grade security systems and data encryption to protect you and guard against unauthorized transactions and access to your personal or financial information."

33. Despite these representations, until approximately March 2015, Venmo failed to implement sufficient safeguards to protect the security, confidentiality, and integrity of consumer information. For example, Venmo failed to provide consumers with security notifications regarding changes to account settings from within the consumer's Venmo account, including informing a consumer that her password or e-mail address had changed, that a new email address

had been added, or that a new device was added to her account. As a result, in some instances, unauthorized users successfully took over consumer accounts, changed the passwords and/or e-mail addresses associated with the accounts, and withdrew funds out of the accounts – all without any notifications to the affected consumers.

34. In addition, due to Venmo's failure to maintain adequate customer support capabilities, as noted above in Paragraph 15, Venmo was often slow to respond to reports of unauthorized transactions.

VENMO'S GRAMM-LEACH-BLILEY ACT VIOLATIONS

35. Respondent is a financial institution, as that term is defined by Section 509(3)(A) of the Gramm-Leach-Bliley ("GLB") Act, 15 U.S.C. § 6809(3)(A), and is subject to the GLB Act. The GLB Act defines a financial institution as "any institution the business of which is engaging in financial activities as described in Section 1843(k) of Title 12 (The Bank Holding Company Act of 1956")." 15 U.S.C. § 6809(3)(A). Among other things, Respondent is significantly engaged in "transferring money," one of the activities listed as financial in nature under the Bank Holding Company Act of 1956, 12 U.S.C. § 1843(k)(A). Respondent is also significantly engaged in data processing and transmission, financial activities listed by the Consumer Financial Protection Bureau ("CFPB") in Regulation Y, 12 C.F.R. § 225.28(b)(14), as covered by GLB. Respondent collects nonpublic personal information, as defined by 16 C.F.R. § 313.3(n). Because Respondent is a financial institution that collects nonpublic personal information, during the relevant time period it was subject to the requirements of the GLB Privacy Rule, 16 C.F.R. § 313.1 *et seq.*, and is subject to the requirements of Reg. P, 12 C.F.R. Part 1016, and the GLB Safeguards Rule, 16 C.F.R. § 314.1 *et seq.*

Privacy Rule and Reg. P

36. The Privacy Rule, which implements Sections 501-503 of the GLB Act, 15 U.S.C. §§ 6801-6803, was promulgated by the Commission on May 24, 2000, and became effective on July 1, 2001. *See* 16 C.F.R. Part 313. Since the enactment of the Dodd-Frank Act on July 21, 2010, the CFPB became responsible for implementing the Privacy Rule, and accordingly promulgated the Privacy of Consumer Financial Information, Regulation P, 12 C.F.R. Part 1016 ("Reg. P"), which became effective on October 28, 2014. Accordingly, Respondent's conduct is governed by the Privacy Rule prior to October 28, 2014, and by Reg. P after that date. The GLB Act authorizes both the CFPB and the FTC to enforce Reg. P. 15 U.S.C. § 6805.

37. Both Reg. P and the Privacy Rule require financial institutions to provide customers with an initial and annual privacy notice. Among other things:

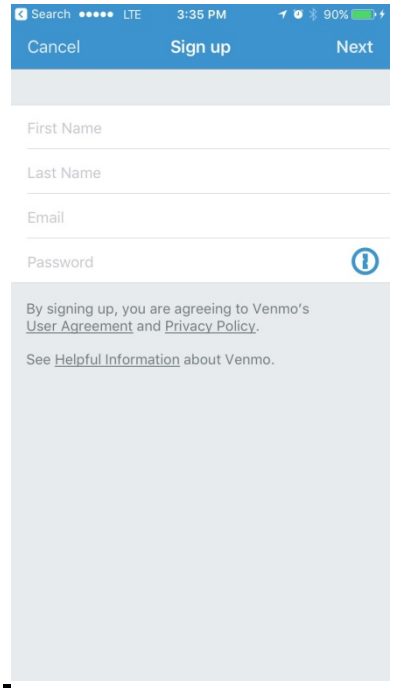
a. These privacy notices must be "clear and conspicuous." 16 C.F.R. §§ 313.4 and 313.5; 12 C.F.R. §§ 1016.4 and 1016.5. "Clear and conspicuous means that a notice is reasonably understandable and designed to call attention to the nature and significance of the information in the notice." 16 C.F.R. § 313.3(b)(1); 12 C.F.R. § 1016.3(b)(1);

b. These privacy notices must "accurately reflect[] [the financial institution's] privacy policies and practices." 16 C.F.R. § 313.4 and 313.5; 12 C.F.R. §§ 1016.4 and 1016.5. They must include specified elements, including the categories of nonpublic personal information the financial institution collects and discloses, the categories of third parties to whom the financial institution discloses the information, and the security and confidentiality policies of the financial institution. 16 C.F.R. § 313.6; 12 C.F.R. § 1016.6; and

c. These privacy notices must be provided "so that each consumer can reasonably be expected to receive actual notice." 16 C.F.R. § 313.9; 12 C.F.R. § 1016.9. For example, for the consumer who conducts transactions electronically, a financial institution may require the consumer to acknowledge receipt of the initial notice as a necessary step to obtaining the financial product or service. 16 C.F.R. § 313.9(b)(1)(iii); 12 C.F.R. § 1016.9(b)(1)(iii).

38. Venmo has failed to comply with the requirements described in Paragraph 37 since it began providing its mobile payment service in 2011. Specifically:

a. Venmo failed to provide a clear and conspicuous initial privacy notice to its customers. Rather, at all times relevant to the complaint, users of Venmo's mobile applications have seen a screen during the signup process the same as or similar to the screenshot depicted below:



This screen informs users that "[b]y signing up, you are agreeing to Venmo's User Agreement and Privacy Policy." As shown in the screenshot above, this disclosure is printed in grey text on a light grey background and does not provide a clear and conspicuous initial privacy notice designed to call attention to the

nature and significance of the information in the notice, as required by the Privacy Rule and Reg. P;

b. Venmo's privacy notice is not accurate, as required by the Privacy Rule and Reg P. Venmo represents in its Privacy Policy that it shares a user's personal information with the user's "social web, if [the user's] Venmo account transactions are designated as 'public' or friends-only payments . . . ." In fact, as described in Paragraphs 17-23, Venmo shares a consumer's personal information by default with "everyone on the Internet," including persons who do not have a Venmo account, and not just members of the consumer's "social web"; and

c. Venmo has failed to deliver the initial privacy notice so that each customer could reasonably be expected to receive actual notice, as required by the Privacy Rule and Reg P. For example, users of Venmo's mobile app may click on a link to Venmo's Privacy Policy to find a description of the company's practices regarding the collection and sharing of personal information, including personal financial information, but Venmo does not require customers to acknowledge receipt of an initial privacy notice as a necessary step to obtaining a particular financial product or service.

Safeguards Rule

39. The Safeguards Rule, which implements Section 501(b) of the GLB Act, 15 U.S.C. § 6801(b), requires financial institutions to protect the security, confidentiality, and integrity of customer information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards, including: (1) designating one or more employees to coordinate the information security program; (2) identifying reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information, and assessing the sufficiency of any safeguards in place to control those risks; (3) designing and implementing information safeguards to control the risks identified through risk assessment, and regularly testing or otherwise monitoring the effectiveness of the safeguards' key controls, systems, and procedures; (4) overseeing service providers and requiring them by contract to protect the security and confidentiality of customer information; and (5) evaluating and adjusting the information security program in light of the results of testing and monitoring, changes to the business operation, and other relevant circumstances.16 C.F.R. §§ 314.3 and 314.4. Violations of the Safeguards Rule are enforced through the FTC Act. 15 U.S.C. § 6805(a)(7).

40. Until approximately March 2015, Venmo failed to comply with the requirements described in Paragraph 39. Specifically,

a. Through at least August 2014, Venmo failed to have a written information security program;

b. Until at least September 2014, Venmo failed to assess reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information; and

c. Until approximately March 2015, Venmo failed to implement basic safeguards to protect the security, confidentiality, and integrity of consumer information, including:

1) Failing to provide security notifications to consumers, such as notifications that a consumer's password or e-mail address has changed, or that a new device was added to the consumer's account; and

2) Failing to maintain adequate customer support to timely investigate and respond to users' reports concerning account compromise or unauthorized transactions.

VIOLATIONS OF THE FTC ACT

COUNT I

41. Through the means described in Paragraphs 4 – 16, Respondent, through Venmo, has represented, directly or indirectly, expressly or by implication, that money is credited to a consumer's Venmo account and can be transferred to an external bank account.

42. In fact, in numerous instances in which Respondent has made the representation set forth in Paragraph 41, Respondent has failed to disclose or disclose adequately to consumers that funds could be frozen or removed because Respondent has not yet approved the underlying transaction. This additional information would be material to consumers in their decision to use Respondent's payment and social networking service.

43. Respondent's failure to disclose or disclose adequately the material information described in Paragraph 42, in light of the representation described in Paragraph 41, is a deceptive act or practice.

COUNT II

44. As described in Paragraphs 17 – 24, 27, and 30 – 31, Respondent, through Venmo, has represented, directly or indirectly, expressly or by implication, that through the Default Audience Setting, consumers can restrict the visibility of future transactions to specific groups, such as "Participants Only" or "Friends."

45. Respondent failed to disclose, or failed to disclose adequately, that the Default Audience Setting does not ensure that future transactions are visible only to friends or to the participants of the transaction, as described in Paragraphs 25 – 26. This fact would be material to consumers in their decision to use Respondent's services.

46. Respondent's failure to disclose or disclose adequately the material information described in Paragraph 45, in light of the representation set forth in Paragraph 44, is a deceptive act or practice.

COUNT III

47. As described in Paragraphs 17 – 24, 28, and 30 – 31, Respondent, through Venmo, has represented, directly or indirectly, expressly or by implication, that through the Individual Audience Setting, consumers can restrict the visibility of any single transaction to specific groups, such as "Participants Only" or "Friends."

48. Respondent failed to disclose, or failed to disclose adequately, that the Individual Audience Setting does not ensure that any single transaction is visible only to friends or to the participants of the transaction, as described in Paragraph 29. This fact would be material to consumers in their decision to use Respondent's services.

49. Respondent's failure to disclose or disclose adequately the material information described in Paragraph 48, in light of the representation set forth in Paragraph 47, is a deceptive act or practice.

COUNT IV

50. As described in Paragraph 32, Respondent, through Venmo, has represented, directly or indirectly, expressly or by implication, that Respondent protected consumers' financial information with "bank grade security systems."

51. In fact, as described in Paragraphs 33 – 34, Respondent did not secure consumers' financial information with "bank grade security systems." Therefore, the representation set forth in Paragraph 50 is false or misleading.

VIOLATION OF THE PRIVACY RULE AND REG. P
COUNT V

52. As described in Paragraphs 36 – 37, the Privacy Rule and Reg. P require financial institutions to provide customers with a clear and conspicuous initial privacy notice that accurately reflects the financial institution's privacy policies and practices, and to deliver the privacy notice so that each customer could reasonably be expected to receive actual notice.

53. Respondent is a financial institution, as defined in Section 509(3)(A) of the GLB Act, 15 U.S.C. § 6809(3)(A).

54. As described in Paragraph 38, Respondent, through Venmo, did not provide users with a clear and conspicuous initial privacy notice. Therefore, Respondent violated the Privacy Rule, 16 C.F.R. § 313.4(a), and Reg. P, 12 C.F.R. § 1016.4.

55. As described in Paragraph 38, Respondent, through Venmo, has disseminated an initial privacy notice that does not accurately reflect its policies and practices in violation of the Privacy Rule, 16 C.F.R. § 313.4(a), and Reg. P, 12 C.F.R. § 1016.4(a).

56. As described in Paragraph 38, Respondent, through Venmo, failed to deliver the initial privacy notice so that each customer could reasonably be expected to receive actual notice. Therefore, Respondent violated the Privacy Rule, 16 C.F.R. § 313.9, and Reg. P, 12 C.F.R. § 1016.9.

VIOLATION OF THE SAFEGUARDS RULE
COUNT VI

57. As described in Paragraph 39, the Safeguards Rule requires financial institutions to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information and then design and implement information safeguards to control the risks identified through the risk assessment.

58. Respondent is a financial institution, as defined in Section 509(3)(A) of the GLB Act, 15 U.S.C. § 6809(3)(A).

59. As set forth in Paragraph 40, Respondent, through Venmo, failed to have a written comprehensive information security program until approximately August 2014;

60. As set forth in Paragraph 40, Respondent, through Venmo, failed to assess reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information until approximately September 2015; and

61. As set forth in Paragraph 40, Respondent, through Venmo, failed to implement safeguards to protect the security, confidentiality, and integrity of consumer information until at least March 2015.

62. Therefore, the conduct set forth in Paragraphs 59 – 61 is a violation of the Safeguards Rule, 16 C.F.R. § 314.4.

63. The acts and practices of Respondent as alleged in this complaint constitute unfair or deceptive acts or practices in or affecting commerce in violation of Section 5(a) of the FTC Act.

THEREFORE, the Federal Trade Commission this twenty-third day of May, 2018, has issued this complaint against Respondent.

By the Commission.

Janice Podoll Frankle
Acting Secretary

SEAL: