

Complaint

IN THE MATTER OF

PAYPAL, INC.

CONSENT ORDER, ETC. IN REGARD TO ALLEGED VIOLATIONS OF
SECTION 5 OF THE FEDERAL TRADE COMMISSION ACT, THE
GRAMM-LEACH-BLILEY ACT, THE PRIVACY RULE, REGULATION P,
AND THE SAFEGUARDS RULE

Docket No. C-4651; File No. 162 3102
Complaint, May 23, 2018 – Decision, May 23, 2018

This consent order addresses PayPal, Inc.’s peer-to-peer payment service, Venmo, that incorporates a social networking component through a social “news feed” that shares information about a consumer’s Venmo transactions. The complaint alleges that PayPal, through its operation of Venmo, has violated Section 5 of the FTC Act and the Gramm-Leach-Bliley Act’s Privacy and Safeguards Rules. The consent order prohibits PayPal from making misrepresentations regarding material restrictions, limitations, or conditions to use any payment and social networking service.

Participants

For the *Commission*: Gregory A. Ashe, Cora Han, Ben Rossen
and Lisa Rothfarb.

For the *Respondent*: Eric Mogilnicki, Covington & Burling
LLP.

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:

Complaint

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.

Complaint

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.

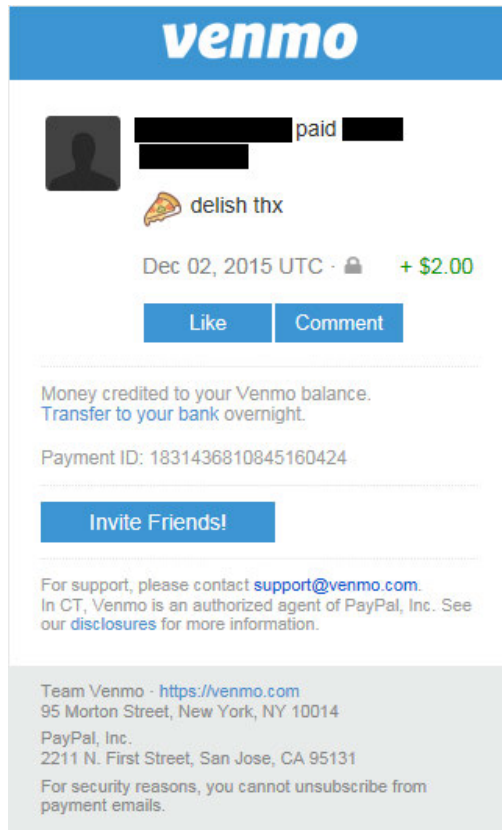
8. As Venmo explains prominently on its website and in mobile application stores, consumers can use the service for a variety of purposes including to “make purchases” and that they can use the service “with anyone.” For example, at various times, the “How it works” page of the Venmo website has stated 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:

Complaint



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.”

Complaint

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

Complaint

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.

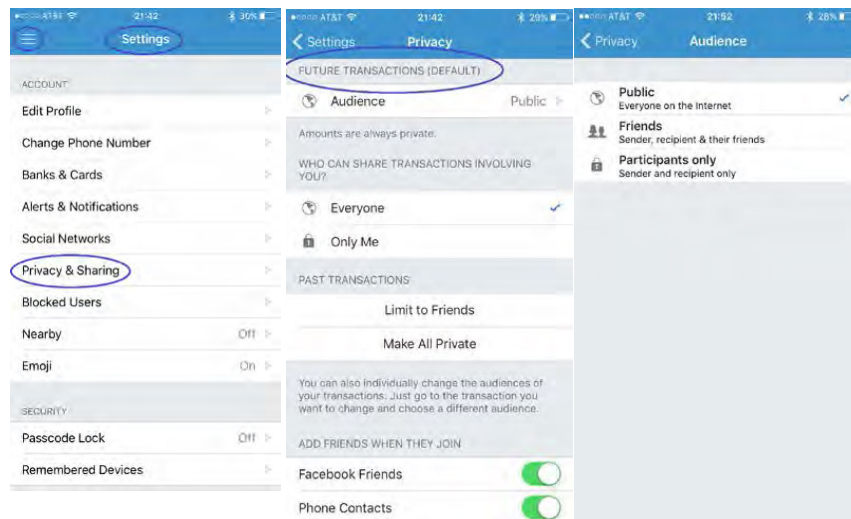
18. Consumers who do not want to share their Venmo transactions may restrict the visibility of their transactions through privacy settings available in a “Settings” menu or by configuring settings for an individual transaction.

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

Complaint

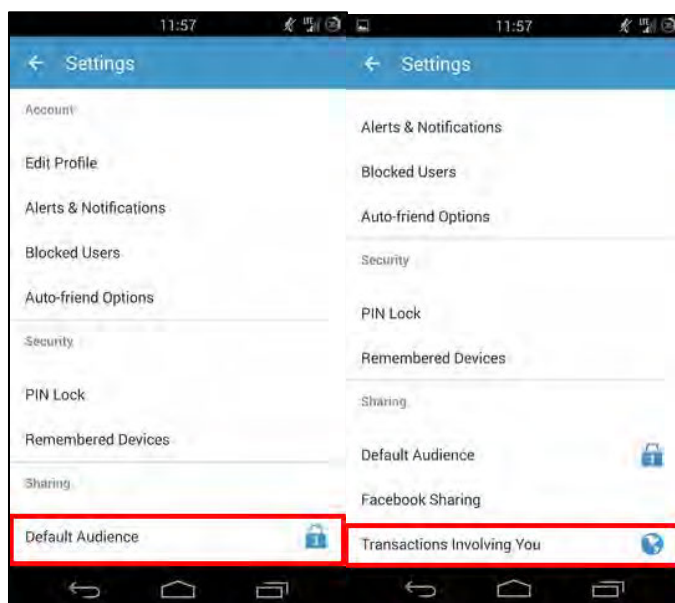
consumer must change two similarly labeled settings. The first setting in this menu limits the “default audience” for “future transactions” (hereinafter, the “Default Audience Setting”). A second setting, described in more detail below, controls “who can share transactions involving” the Venmo user (hereinafter, 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?”

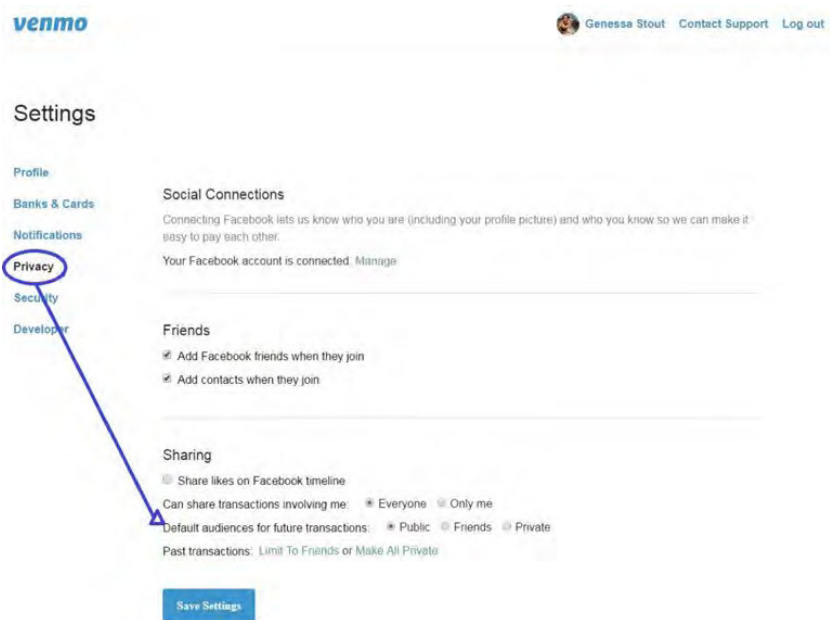


21. On Venmo’s Android App, the privacy settings menu appears the same or similar to the screenshots depicted below:

Complaint



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



Complaint

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

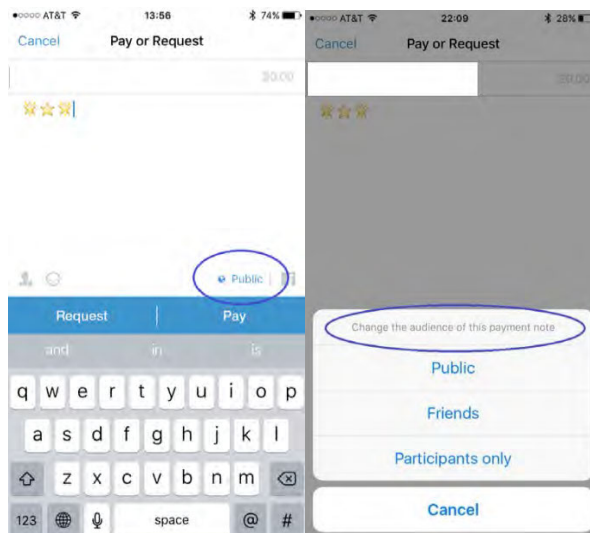
Complaint

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:



Complaint

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).

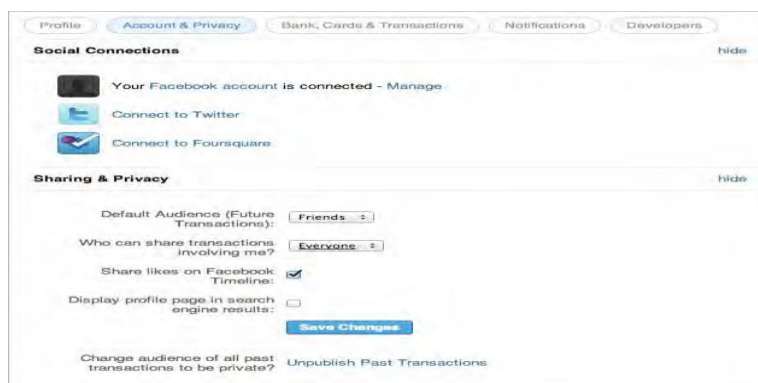
30. Venmo has never informed consumers that the Transaction Sharing Setting permits retroactive changes to the visibility of a transaction, even where one participant has specifically intended for a transaction to be private. In fact, Venmo exacerbates these problems by incorrectly describing its privacy 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/](https://web/20150525161659/https://venmo.com/))
- Navigate to **Account -> Account & Privacy -> Sharing & Privacy -> Edit**
- Choose your desired settings
- **Save**

Complaint



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

Complaint

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

Complaint

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.

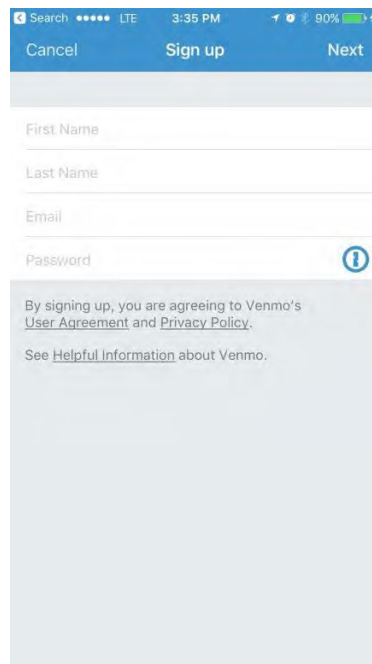
37. Both Reg. P and the Privacy Rule require financial institutions to provide customers with an initial and annual privacy notice. Among other things:

- 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).

Complaint

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;

Complaint

- 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

Complaint

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:
 - i 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
 - ii 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

Complaint

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.

Complaint

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,

Complaint

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).

Decision and Order

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.

DECISION

The Federal Trade Commission (“Commission”) initiated an investigation of certain acts and practices of Respondent named in the caption. The Commission’s Bureau of Consumer Protection (“BCP”) prepared and furnished to Respondent a draft Complaint. BCP proposed to present the draft Complaint to the Commission for its consideration. If issued by the Commission, the draft

Decision and Order

Complaint would charge Respondent with violation of the Federal Trade Commission Act.

Respondent and BCP thereafter executed an Agreement Containing Consent Order (“Consent Agreement”). The Consent Agreement includes: 1) statements by Respondent that it neither admits nor denies any of the allegations in the Complaint, except as specifically stated in this Decision and Order, and that only for purposes of this action, it admits the facts necessary to establish jurisdiction; and 2) waivers and other provisions as required by the Commission’s Rules.

The Commission considered the matter and determined that it had reason to believe that Respondent has violated the Federal Trade Commission Act, and that a Complaint should issue stating its charges in that respect. The Commission accepted the executed Consent Agreement and placed it on the public record for a period of 30 days for the receipt and consideration of public comments. The Commission duly considered the comments received from interested persons pursuant to Commission Rule 2.34, 16 C.F.R. § 2.34. Now, in further conformity with the procedure prescribed in Commission Rule 2.34, the Commission issues its Complaint, makes the following Findings, and issues the following Order:

FINDINGS

1. Respondent PayPal, Inc., operating as Venmo, is a Delaware corporation with its principal office or place of business at 2211 North First Street, San Jose, California 95131.
2. The Commission has jurisdiction over the subject matter of this proceeding and over Respondent, and the proceeding is in the public interest.

Decision and Order

DEFINITIONS

For purposes of this Order, the following definitions apply:

- A. “Clearly and conspicuously” means that a required disclosure is difficult to miss (*i.e.*, easily noticeable) and easily understandable by ordinary consumers, including in all of the following ways:
1. In any communication that is solely visual or solely audible, the disclosure must be made through the same means through which the communication is presented. In any communication made through both visual and audible means, such as a television advertisement, the disclosure must be presented simultaneously in both the visual and audible portions of the communication even if the representation requiring the disclosure (“triggering representation”) is made through only one means.
 2. A visual disclosure, by its size, contrast, location, the length of time it appears, and other characteristics, must stand out from any accompanying text or other visual elements so that it is easily noticed, read, and understood.
 3. An audible disclosure, including by telephone or streaming video, must be delivered in a volume, speed, and cadence sufficient for ordinary consumers to easily hear and understand it.
 4. In any communication using an interactive electronic medium, such as the Internet or software, the disclosure must be unavoidable.
 5. The disclosure must use diction and syntax understandable to ordinary consumers and must appear in each language in which the triggering representation appears.

Decision and Order

6. The disclosure must comply with these requirements in each medium through which it is received, including all electronic devices and face-to-face communications.
 7. The disclosure must not be contradicted or mitigated by, or inconsistent with, anything else in the communication.
 8. When the representation or sales practice targets a specific audience, such as children, the elderly, or the terminally ill, “ordinary consumers” includes reasonable members of that group.
- B. “Close proximity” means that the disclosure is very near the triggering representation. For example, a disclosure made through a hyperlink, pop-up, interstitial, or other similar technique is not in close proximity to the triggering representation.
- C. “Covered information” means information from or about a User, including: (a) a first and last name; (b) a physical address; (c) an email address or other online contact information, such as a user identifier or a screen name; (d) a telephone number; (e) a Social Security number; (f) a financial institution account number; (g) credit or debit card information; or (h) transaction information.
- D. “Privacy setting” shall include any control or setting provided by Respondent that allows a user to limit or restrict which individuals or entities can access or view covered information.
- E. “Respondent” means PayPal, Inc. and its successors and assigns.
- F. “Transaction information” means information from or about a Payment and Social Networking Service transaction, including (a) the participants to the transaction; (b) the date of the transaction; or (c) any

Decision and Order

accompanying message or other descriptor related to the transaction.

- G. “User” means any person with a Payment and Social Networking Service account.
- H. “Payment and Social Networking Service” means any app or website owned and operated by Respondent that allows consumers to make payments and to share information regarding such payments with other Users through a social network owned and operated by Respondent.
- I. “Venmo” means the wholly or partially owned subsidiary, unincorporated division or business unit, or affiliate of PayPal, Inc., however denominated, that operates the Payment and Social Networking Service currently branded as Venmo.

ORDER**I. PROHIBITED MISREPRESENTATIONS**

IT IS ORDERED that Respondent, and Respondent’s officers, agents, employees, and attorneys, and all other persons in active concert or participation with any of them, who receive actual notice of this Order, whether acting directly or indirectly, in connection with the advertising, promotion, offering for sale, sale, or use of any Payment and Social Networking Service must not misrepresent or assist others in misrepresenting, expressly or by implication:

- A. Any material restriction, limitation, or condition to use any Payment and Social Networking Service; and
- B. The extent to which Respondent, in connection with any Payment and Social Networking Service, protects the privacy, confidentiality, security, or integrity of any covered information, including:

Decision and Order

1. The extent to which a consumer may exercise control over the disclosure of any covered information from or about a User and the steps a User must take to implement any such controls; and
2. The extent to which Respondent implements or adheres to a particular level of security.

II. REQUIRED DISCLOSURES**IT IS FURTHER ORDERED** that:

- A. Within one hundred and fifty (150) days of the effective date of this Order, Respondent, and Respondent's officers, agents, employees, and attorneys, and all other persons in active concert or participation with any of them, who receive actual notice of this Order, whether acting directly or indirectly, when making any representation through any Payment and Social Networking Service, expressly or by implication, about the availability of funds to be transferred or withdrawn to a bank account (1) must disclose, clearly and conspicuously, and in close proximity to such representation (a) that the transaction is subject to review and (b) the fact, if true, that funds could be frozen or removed as a result of transaction reviews performed during the bank transfer or withdrawal process, and (2) the representation must not be otherwise misleading.
- B. Respondent must issue a notice to Users, within one hundred and fifty (150) days of the effective date of this Order as follows: (i) for Users who have installed a Payment and Social Networking Service as an app, through the app such that the notice appears when the User next opens the app or (ii) for Users who have not installed a Payment and Social Networking Service as an app, through a text message, email, or other communication sufficient to provide clear and conspicuous notice prior to the User's next transaction.

Decision and Order

The notice shall disclose, clearly and conspicuously, and separate and apart from any “privacy policy,” “terms of use,” “end user license agreement,” or similar document, the fact, if true, that when a User attempts to transfer or withdraw funds to a bank account, Respondent (1) will perform transaction reviews, and (2) based on such review, may (i) block or delay the transfer or withdrawal, and/or (ii) reverse a payment transaction.

III. ADDITIONAL PRIVACY DISCLOSURES

IT IS FURTHER ORDERED that, within one hundred and fifty (150) days of the effective date of this Order, and continuing thereafter, Respondent and Respondent’s officers, agents, employees, and attorneys, and all other persons in active concert or participation with any of them, who receive actual notice of this Order, whether acting directly or indirectly, in connection with any Payment or Social Networking Service, must clearly and conspicuously disclose to each User, through the Payment and Social Networking Service, and separate and apart from any “privacy policy,” “terms of use,” “blog,” “helpful information” page, or similar document: (1) how the User’s transaction information will be shared with other Users; and (2) how the User can use privacy settings to limit or restrict the visibility or sharing of the User’s transaction information on the Payment and Social Networking Service. For Users that have already created an account when this disclosure is first issued, this disclosure must occur at or immediately prior to the time that the User next engages in a transaction through the Payment and Social Networking Service. For Users that have not created an account when this disclosure is first issued, this disclosure must occur at the time the User opens an account. This disclosure must not contain any other information.

IV. GLB RULE PROVISIONS

IT IS FURTHER ORDERED that Respondent, and Respondent’s officers, agents, employees and attorneys, and all other persons in active concert or participation with any of them, who receive actual notice of this Order, whether acting directly or

Decision and Order

indirectly, in connection with any Payment and Social Networking Service, are hereby permanently restrained and enjoined from violating any provision of:

- A. The Privacy of Consumer Financial Information Rule (Regulation P), 12 C.F.R. Part 1016; or
- B. The Standards for Safeguarding Consumer Information Rule, 16 C.F.R. Part 314.

In the event that any of the statutory sections or rules identified in this Part are hereafter amended or modified, compliance with that statutory section or rule as so amended or modified shall not be a violation of this Order.

V. BIENNIAL ASSESSMENT REQUIREMENTS

IT IS FURTHER ORDERED that Respondent, and its successors and assigns, in connection with their compliance with Section IV(A) and (B) of this Order, shall obtain initial and biennial assessments and reports (“Assessments”) of the Venmo Payment and Social Networking Service from a qualified, objective, independent third-party professional, using procedures and standards generally accepted in the profession. The reporting period for the Assessments shall cover: (1) the first one hundred and eighty (180) days after service of the Order for the initial Assessment, and (2) each two-year period thereafter for ten (10) years after service of this Order for the biennial Assessments. Each Assessment shall:

- A. Set forth the specific administrative, technical, and physical safeguards that Respondent has implemented and maintained during the reporting period;
- B. Explain how such safeguards are appropriate to Respondent’s size and complexity, the nature and scope of Respondent’s activities, and the sensitivity of the covered information collected from or about consumers;

Decision and Order

- C. Explain how the safeguards that have been implemented meet or exceed the protections required by Section IV(B) of this Order; and
- D. Certify that Respondent's security program(s) is operating with sufficient effectiveness to provide reasonable assurance that the confidentiality, security, and integrity of covered information is protected and has so operated throughout the reporting period.

Each Assessment must be completed within 60 days after the end of the reporting period to which the Assessment applies. The Assessment must be obtained from a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession. A professional qualified to prepare such Assessments must be: an individual qualified as a Certified Information System Security Professional (CISSP) or as a Certified Information Systems Auditor (CISA); an individual holding Global Information Assurance Certification (GIAC) from the SANS Institute; or a qualified individual or entity approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission.

Respondent must submit the initial Assessment to the Commission within 10 days after the Assessment has been completed. Respondent must retain all subsequent biennial Assessments, at least until the Order terminates. Respondent must submit any biennial Assessments to the Commission within 10 days of a request from a representative of the Commission.

VI. ACKNOWLEDGMENTS OF THE ORDER

IT IS FURTHER ORDERED that Respondent obtains acknowledgments of receipt of this Order:

- A. Respondent, within 10 days after the effective date of this Order, must submit to the Commission an acknowledgment of receipt of this Order sworn under penalty of perjury.

Decision and Order

- B. For 20 years after the issuance date of this Order, Respondent must deliver a copy of this Order to: (1) all principals, officers, directors, and LLC managers and members; (2) all employees, agents, and representatives who participate in conduct related to the subject matter of the Order; and (3) any business entity resulting from any change in structure as set forth in the Provision titled Compliance Reports and Notices. Delivery must occur within 10 days after the effective date of this Order for current personnel. For all others, delivery must occur before they assume their responsibilities.
- C. From each individual or entity to which Respondent delivered a copy of this Order, Respondent must obtain, within 60 days, a signed and dated acknowledgment of receipt of this Order.

VII. COMPLIANCE REPORTS AND NOTICES

IT IS FURTHER ORDERED that Respondent make timely submissions to the Commission:

- A. One year after the issuance date of this Order, Respondent must submit a compliance report, sworn under penalty of perjury, in which Respondent must: (a) identify the primary physical, postal, and email address and telephone number, as designated points of contact, which representatives of the Commission, may use to communicate with Respondent; (b) identify all of Respondent's businesses by all of their names, telephone numbers, and physical, postal, email, and Internet addresses; (c) describe the activities of each business, including the goods and services offered, the means of advertising, marketing, and sales; (d) describe in detail whether and how Respondent is in compliance with each Provision of this Order, including a discussion of all of the changes Respondent made to comply with the Order; and (e) provide a copy of each Acknowledgment of the Order

Decision and Order

obtained pursuant to this Order, unless previously submitted to the Commission.

- B. Respondent must submit a compliance notice, sworn under penalty of perjury, within 14 days of any change in the following: (a) any designated point of contact; or (b) the structure of Respondent or any entity that Respondent has any ownership interest in or controls directly or indirectly that may affect compliance obligations arising under this Order, including: creation, merger, sale, or dissolution of the entity or any subsidiary, parent, or affiliate that provides a Payment and Social Networking Service.
- C. Respondent must submit notice of the filing of any bankruptcy petition, insolvency proceeding, or similar proceeding by or against Respondent within 14 days of its filing.
- D. Any submission to the Commission required by this Order to be sworn under penalty of perjury must be true and accurate and comply with 28 U.S.C. § 1746, such as by concluding: “I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on: _____” and supplying the date, signatory’s full name, title (if applicable), and signature.
- E. Unless otherwise directed by a Commission representative in writing, all submissions to the Commission pursuant to this Order must be emailed to DEbrief@ftc.gov or sent by overnight courier (not the U.S. Postal Service) to: Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin: In re PayPal.

Decision and Order

VIII. RECORDKEEPING

IT IS FURTHER ORDERED that Respondent must create certain records for 20 years after the issuance date of the Order, and retain each such record for 5 years, unless otherwise specified below. Specifically, Respondent must create and retain the following records:

- A. accounting records showing the revenues from all Payment and Social Networking Services sold;
- B. personnel records showing, for each person providing services in relation to any aspect of the Order, whether as an employee or otherwise, that person's: name; addresses; telephone numbers; job title or position; dates of service; and (if applicable) the reason for termination;
- C. copies or records of all consumer complaints regarding any Payment and Social Networking Service, whether received directly or indirectly, such as through a third party, and any response;
- D. all records necessary to demonstrate full compliance with each provision of this Order, including all submissions to the Commission;
- E. a copy of each unique Payment and Social Networking Service advertisement or other marketing material making a representation subject to this Order; and
- F. for 3 years after the date of preparation of each Assessment required by this Order, all materials relied upon to prepare the Assessment, whether prepared by or on behalf of Respondent, including all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, and any other materials concerning Respondent's compliance with related Provisions of this Order, for the compliance period covered by such Assessment.

Decision and Order

IX. COMPLIANCE MONITORING

IT IS FURTHER ORDERED that, for the purpose of monitoring Respondent's compliance with this Order:

- A. Within 10 days of receipt of a written request from a representative of the Commission, Respondent must submit additional compliance reports or other requested information, which must be sworn under penalty of perjury, and produce records for inspection and copying.
- B. For matters concerning this Order, representatives of the Commission are authorized to communicate directly with Respondent. Respondent must permit representatives of the Commission to interview anyone affiliated with Respondent who has agreed to such an interview. The interviewee may have counsel present.
- C. The Commission may use all other lawful means, including posing through its representatives as consumers, suppliers, or other individuals or entities, to Respondent or any individual or entity affiliated with Respondent, without the necessity of identification or prior notice. Nothing in this Order limits the Commission's lawful use of compulsory process, pursuant to Sections 9 and 20 of the FTC Act, 15 U.S.C. §§ 49, 57b-1.

X. ORDER EFFECTIVE DATES

IT IS FURTHER ORDERED that this Order is final and effective upon the date of its publication on the Commission's website (ftc.gov) as a final order. This Order will terminate on May 23, 2038, or 20 years from the most recent date that the United States or the Commission files a complaint (with or without an accompanying settlement) in federal court alleging any violation of this Order, whichever comes later; *provided, however*, that the filing of such a complaint will not affect the duration of:

Analysis to Aid Public Comment

- A. Any Provision in this Order that terminates in less than 20 years;
- B. This Order's application to any Respondent that is not named as a defendant in such complaint; and
- C. This Order if such complaint is filed after the Order has terminated pursuant to this Provision.

Provided, further, that if such complaint is dismissed or a federal court rules that Respondent did not violate any provision of the Order, and the dismissal or ruling is either not appealed or upheld on appeal, then the Order will terminate according to this Provision as though the complaint had never been filed, except that the Order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

By the Commission.

ANALYSIS OF CONSENT ORDER TO AID PUBLIC COMMENT

The Federal Trade Commission ("Commission") has accepted, subject to final approval, an agreement containing a consent order from PayPal, Inc. ("PayPal").

The proposed consent order has been placed on the public record for thirty (30) days for receipt of comments by interested persons. Comments received during this period will become part of the public record. After 30 days, the Commission will again review the agreement and the comments received, and will decide whether it should withdraw from the agreement and take appropriate action or make final the agreement's proposed order.

Analysis to Aid Public Comment

This matter involves Venmo, a peer-to-peer payment service owned and operated by PayPal. Venmo has offered its peer-to-peer payment service to consumers since 2011, and was acquired by PayPal in 2013. Consumers can use Venmo to transfer money to one another using a mobile application or through a website at www.venmo.com. Venmo's payment service incorporates a social networking component through a social "news feed" that shares information about a consumer's Venmo transactions.

The Commission's proposed complaint alleges that PayPal, through its operation of Venmo, has violated Section 5 of the FTC Act and the Gramm-Leach-Bliley ("GLB") Act's Privacy and Safeguards Rules.

First, the proposed complaint alleges that Venmo has represented to consumers that money is credited to their Venmo account and can be transferred to an external bank account after other Venmo users have sent funds to those consumers, but has failed to disclose, or failed to disclose adequately, that funds could be frozen or removed because Venmo has not yet approved the underlying transaction. As alleged in the proposed complaint, Venmo has made representations to consumers that they have been paid and they can transfer money from Venmo to an external bank account. For example, Venmo has sent users notifications that have stated "Money credited to your Venmo balance. Transfer to your bank overnight." Despite these claims, the proposed complaint alleges that, 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 an external bank account to review the transaction for certain issues. This review has resulted in Venmo delaying the transfer or reversing the transaction in numerous instances.

Second, the proposed complaint alleges that Venmo has failed to disclose material information to consumers about the operation of Venmo's privacy settings. As alleged in the proposed complaint, by default, all Venmo transactions are shared on Venmo's social news feed, which displays the names of the payer and recipient, the date of the transaction, and a message written by the user that initiated the transaction. Venmo offers privacy

Analysis to Aid Public Comment

settings that consumers can use to limit the visibility of their transactions. However, to ensure that all future payments remain private, a consumer must change two similarly labeled settings. The first setting, referred to in the proposed complaint as the “Default Audience Setting,” would lead a reasonable consumer to believe that they can restrict the visibility of their future transactions on the news feed to specific groups, such as “Participants Only” or “Friends.” In fact, however, a consumer must also change a second setting, referred to in the proposed complaint as the “Transaction Sharing Setting,” to ensure that all of her transactions are private. If a consumer fails to restrict this second setting, in some circumstances, transactions will still be published publicly even if the consumer has chosen a “private” default audience.

Venmo also offers a privacy setting to control the visibility of an individual transaction, referred to in the proposed complaint as the “Individual Audience Setting.” The proposed complaint alleges that Venmo failed to disclose, or failed to disclose adequately, that the Individual Audience Setting does not ensure that an individual transaction remains private unless a consumer also separately restricts the Transaction Sharing Setting described above. If a consumer has not changed both settings, there are circumstances where the other participant in the transaction can retroactively change a transaction from private to public.

Third, the proposed complaint alleges that Venmo represented until approximately March 2015 that it protected consumers’ financial information with “bank grade security systems” but in fact failed to implement basic safeguards necessary to secure consumer accounts from unauthorized transactions and did not provide “bank grade security.” For example, Venmo failed to provide consumers with security notifications about changes to account settings from within the consumer’s Venmo account, such as when a consumer’s email address or password had been changed. The proposed complaint alleges that Venmo’s representation that it provided “bank grade security systems” constitutes a deceptive act or practice under Section 5 of the FTC Act.

Analysis to Aid Public Comment

Fourth, the proposed complaint alleges that Venmo violated the GLB Act's Privacy Rule and Regulation P by failing to provide users with a clear and conspicuous initial privacy notice, disseminating an initial privacy notice that does not accurately reflect its policies and practices, and failing to deliver the initial privacy notice so that each customer could reasonably be expected to receive actual notice.

Finally, the proposed complaint alleges that Venmo violated the GLB Act's Safeguards Rule by failing to have a comprehensive written information security program before August 2014, failing to identify 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 before September 2014, and failing to design and implement information safeguards to control the known risks to the security, confidentiality, and integrity of customer information.

The proposed order contains injunctive provisions addressing the alleged deceptive conduct and Rule violations in connection with PayPal's operation of a payment and social networking service. Part I of the proposed order prohibits PayPal from making misrepresentations regarding material restrictions, limitations, or conditions to use any payment and social networking service. It also prohibits misrepresentations about data security and privacy, including misrepresentations regarding the extent of control provided by any privacy settings and the extent to which PayPal implements or adheres to a particular level of security.

Part II of the proposed order requires PayPal, when making any representations through any payment and social networking service about the availability of funds to be transferred or withdrawn to a bank account, to provide clear and conspicuous disclosures that transactions are subject to review and, if true, that funds could be frozen or removed as a result of transaction reviews. Part II also requires PayPal to issue a one-time notice informing current Venmo users that when they attempt to transfer or withdraw funds to a bank account, Venmo will perform

Analysis to Aid Public Comment

transaction reviews and based on such review, may block or delay the transfer or withdrawal, and/or reverse a payment transaction.

Part III of the proposed order requires PayPal to provide clear and conspicuous disclosures to users related to how any payment and social networking service shares transaction information with other users and how a consumer can limit the visibility or sharing of transaction information through privacy settings.

Part IV of the agreement prohibits violations of the GLB Privacy and Safeguards Rules.

Part V requires PayPal to obtain biennial data security assessments for ten years.

Parts VI through IX of the proposed order are reporting and compliance provisions, which include recordkeeping requirements and provisions requiring PayPal to provide information or documents necessary for the Commission to monitor compliance. Part X states that the proposed order will remain in effect for 20 years, with certain exceptions.

The purpose of this analysis is to aid public comment on the proposed order. It is not intended to constitute an official interpretation of the complaint or proposed order, or to modify in any way the proposed order's terms.

Complaint

IN THE MATTER OF

**NORTHROP GRUMMAN CORPORATION
AND
ORBITAL ATK, INC.**CONSENT ORDER, ETC. IN REGARD TO ALLEGED VIOLATIONS OF
SECTION 5 OF THE FEDERAL TRADE COMMISSION ACT AND
SECTION 7 OF THE CLAYTON ACT

*Docket No. C-4652; File No. 181 0005
Complaint, June 5, 2018 – Decision, June 5, 2018*

This consent order addresses the \$7.8 billion acquisition by Northrop Grumman Corporation of certain assets of Orbital ATK, Inc. The complaint alleges that the acquisition, if consummated, would violate Section 7 of the Clayton Act and Section 5 of the Federal Trade Commission Act by lessening the competition in the United States market for missile systems. The consent order requires Northrop to (1) continue to act as a non-discriminatory merchant supplier of Orbital ATK's solid rocket motors ("SRMs") rather than favor its now-vertically integrated missile system business, and (2) protect SRM and missile system competitors' competitively sensitive information from improper use or disclosure.

Participants

For the *Commission*: James E. Southworth.

For the *Respondents*: Thomas O. Barnett and Deborah A. Garza, Covington & Burling LLP; Joseph Krauss, Hogan Lovells US LLP.

COMPLAINT

Pursuant to the Clayton Act and the Federal Trade Commission Act ("FTC Act"), and its authority thereunder, the Federal Trade Commission ("Commission"), having reason to believe that Respondent Northrop Grumman Corporation ("Northrop"), a corporation subject to the jurisdiction of the Commission, has agreed to acquire Orbital ATK, Inc. ("Orbital"), a corporation subject to the jurisdiction of the Commission, in violation of Section 5 of the FTC Act, as amended, 15 U.S.C. § 45, that such acquisition, if consummated, would violate Section 7 of the Clayton Act, as amended, 15 U.S.C. § 18, and Section 5 of