Amber L. Schubert #278696
Sonum Dixit #353395
Of Counsel
AYLSTOCK WITKIN
KREIS & OVERHOLTZ PLC
17 E. Main Street, Suite 200
Pensacola, FL 32502
Tel: 850.202.1010
aschubert@awkolawllp.com
sdixit@awkolawllp.com

Christian Levis (*pro hac vice* forthcoming)
Patricia Zapata Latzer (*pro hac vice* forthcoming)
LOWEY DANNENBERG, P.C.
44 South Broadway, Suite 1100
White Plains, NY 10601
Tel: (914) 997-0500
Fax: (914) 997-0035
clevis@lowey.com
platzer@lowey.com

Anthony M. Christina (*pro hac vice* forthcoming)
LOWEY DANNENBERG, P.C.
One Tower Bridge
100 Front Street, Suite 520
West Conshohocken, PA 19428
Tel: (215) 399-4770
Fax: (914) 997-0035
achristina@lowey.com

Counsel for Plaintiffs and the Proposed Classes

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION

STACEY BORQUEZ, REMI RUNDZIO, and NATHAN OLSON, and LANA NAVA, individually and on behalf of all others similarly situated, Plaintiffs, v. PAYPAL, INC. d/b/a VENMO, Defendant.	Case No.: 5:26-cv-9340 **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiffs Stacey Borquez, Remi Rundzio, Nathan Olson, and Lana Nava, individually and on behalf of all others similarly situated, assert the following class action complaint (the "Complaint") against Defendant PayPal, Inc. d/b/a Venmo ("Defendant" or "PayPal"), based upon personal knowledge, where applicable, information and belief, and the investigation of counsel.

SUMMARY OF ALLEGATIONS

1. Venmo is a peer-to-peer payment platform owned and operated by PayPal. Users can access Venmo via a website and mobile application (collectively, the "Venmo Platform").

2. Tens of millions of Americans use the Venmo Platform for a variety of financial purposes, including, for example, personal banking, sending money to family and friends, splitting rent, paying for goods and services, and settling debts. These activities may and often do reveal, in granular detail, who a person transacts with, how much they spend, and why.

3. Every payment processed through the Venmo Platform generates a record that includes the identity of the sender, the identity of the recipient, the amount paid, and a text "note" in which the user can write and describe the purpose of the transaction. Those notes routinely disclose information that is private in nature, like payments related to medical treatment, legal services, addiction and recovery programs, rent and housing payments, gambling, political and religious donations, romantic and sexual relationships, and countless other intimate details of a person's life.

4. PayPal promised its users that this information would stay private. The Venmo Privacy Statement tells users that "Venmo does not disclose your personal information with third parties for their promotional or marketing purposes,"[1] and that only "public information"[2]—a defined and narrow category—"may also be seen, accessed, reshared or downloaded through Venmo's APIs or third-party services that integrate with our products."[3]

5. PayPal went further. PayPal allows users to default set their transactions to private and also gives users a per-transaction privacy setting. Venmo's Privacy Statement tells users in plain terms what the most protective setting means: if a payment is marked "Private," then "[w]e will not

---

[1] Venmo Privacy Statement (DATE EFFECTIVE: November 17, 2025) (*See* Exhibit A attached to the Complaint).

[2] *Id.*

[3] *Id.*

share the transaction anywhere other than in your personal transactions feed under the Me tab and with the other participant."[4]

6. PayPal reinforced these promises throughout its marketing. It told consumers to "[s]end dollars, not financial details,"[5] assured them that "[e]very transaction in our app is encrypted, so your financial information stays secure whether you're paying a friend or checking out online,"[6] and advertised "[s]ecure transactions."[7]

7. For California users, PayPal made a further, express commitment: "If your Venmo account has a California mailing address, we will not share personal information we collect about you except to the extent permitted under California law."[8]

8. Those assurances were false. Unbeknownst to Plaintiffs and Class Members, PayPal purposefully embedded certain third-party tracking technologies (the "Tracking Technology") into the Venmo Platform.

9. Through that Tracking Technology, PayPal disclosed to, and enabled the interception by, third parties, including, but not limited to, mParticle, Inc. ("mParticle") and Kochava, Inc. ("Kochava") (collectively, the "Third-Party Recipients") of each of the following categories of private financial transaction data and personal information data fields (collectively, "PII"):

A. the sender's full name;

B. the sender's email address;

C. the sender's telephone number;

---

[4] Help Center, Manage your Venmo privacy settings, Venmo, https://help.venmo.com/cs/articles/manage-your-venmo-privacy-settings-vhel351 (last visited August 26, 2026).

[5] Trust & Safety, A safe way to pay and get paid, Venmo, https://venmo.com/about/us/trust-and-safety (last visited August 26, 2026).

[6] *Id.*

[7] Got paid for dinner? Turn it into dessert when you pay with Venmo, Venmo, https://venmo.com/pay/start (last visited August 26, 2026).

[8] Venmo Privacy Statement.

D. the sender's Android Advertising ID ("AAID"), a unique, persistent device identifier;

E. the sender's mParticle ID;

F. the sender's Kochava ID;

G. the identity of the recipient of the transaction;

H. the amount paid; and

I. the note describing the purpose of the transaction.

10. This was not a technical accident or an incidental byproduct of routing a payment. PayPal chose to install the Tracking Technology, chose which screens and events it would fire on and collect, and chose which data fields it would transmit. Only PayPal could configure those transmissions.

11. Nor was the disclosed information anonymous or aggregated. PayPal transmitted the transaction data alongside directly identifying information—name, email address, and telephone number—and alongside persistent identifiers, including the AAID, mParticle ID, and Kochava ID, that exist for the express purpose of following a specific individual across applications, websites, and devices over time. The Third-Party Recipients were not prohibited from using this information for their own purposes, including enriching the commercial profiles they maintain about individuals, as well as the value of their other products.

12. The PII and transaction data PayPal disclosed to third parties are quintessentially private financial information subject to the Gramm-Leach-Bliley Act ("GLBA"). PayPal is a financial institution governed by the GLBA. The Venmo Privacy Statement is delivered to consumers in the form prescribed for financial privacy notices under the GLBA.

13. In the Venmo Privacy Statement, PayPal represents that it does not share personal information with "nonaffiliates"—defined as "[c]ompanies not related by common ownership or

control" that "can be financial and nonfinancial companies"—for those nonaffiliates to market to the consumer, and that consumers need not limit such sharing because "[w]e don't share."[9]

14. Plaintiffs and Class Members did not consent to the disclosure or interception of their private transaction data and PII, nor could they. The Tracking Technology operates invisibly, in the background. No disclosure anywhere in the Venmo Platform told users that their payment amounts, counterparties, and transaction notes would be routed to third-party data companies. However, that is exactly what happened for tens of millions of Venmo users.

PARTIES

A. Plaintiffs

15. Plaintiff Stacey Borquez ("Plaintiff Borquez") is a citizen and resident of Thousand Oaks, California.

16. Plaintiff Borquez has a Venmo account.

17. Plaintiff Borquez used the Venmo Platform mobile application on her personal iPhone device to send and receive monetary payments for personal and work-related reasons.

18. Plaintiff Borquez also has the Venmo-branded debit card and credit card, which she frequently uses to make personal transactions.

19. To open and use a Venmo account, Plaintiff Borquez was required to provide the Venmo Platform with her full name, email address, telephone number, and financial banking account information.

20. Plaintiff Borquez's Venmo account and/or individual transactions were set to "Private," meaning that, according to PayPal's own representations, PayPal would "not share the transaction anywhere other than in your personal transactions feed under the Me tab and with the other participant."[10]

---

[9] Venmo Privacy Statement.

[10] Help Center, Manage your Venmo privacy settings, Venmo, https://help.venmo.com/cs/articles/manage-your-venmo-privacy-settings-vhel351 (last visited August 26, 2026).

21. Plaintiff Borquez read and relied on PayPal's representations regarding the privacy and security of the Venmo Platform, including Venmo's in-application privacy settings and Venmo's marketing representations that transactions are encrypted and secure, before providing Plaintiff Borquez's information to PayPal and before transacting on the Venmo Platform.

22. Plaintiff Borquez used the Venmo Platform extensively, and many of her monetary transactions took place on the Venmo Platform. Plaintiff Borquez had an expectation of privacy with her account set to private. Like other Class Members, Plaintiff Borquez was not clearly and conspicuously informed that even setting her account to private would not prevent her information from being shared with third parties.

23. Unbeknownst to Plaintiff Borquez, PayPal disclosed, and the Third-Party Recipients intercepted and recorded, Plaintiff Borquez's PII, which includes transaction information such as recipient details and notes associated with each transaction.

24. Plaintiff Remi Rundzio ("Plaintiff Rundzio") is a citizen and resident of Westminster, California.

25. Plaintiff Rundzio has a Venmo account.

26. Plaintiff Rundzio used the Venmo Platform mobile application on his personal Android device to send and receive monetary payments for personal reasons.

27. To open and use a Venmo account, Plaintiff Rundzio was required to provide PayPal with his full name, email address, telephone number, and financial banking account information.

28. Plaintiff Rundzio sent transactions on the Venmo Platform that were set to "Private," meaning that, according to PayPal's own representations, PayPal would "not share the transaction anywhere other than in your personal transactions feed under the Me tab and with the other participant."[11]

---

[11] Help Center, Manage your Venmo privacy settings, Venmo, https://help.venmo.com/cs/articles/manage-your-venmo-privacy-settings-vhel351 (last visited August 26, 2026).

29. Plaintiff Rundzio read and relied on PayPal's representations regarding the privacy and security of the Venmo Platform, including Venmo's in-application privacy settings and Venmo's marketing representations that transactions are encrypted and secure, before providing Plaintiff Rundzio's information to PayPal and before transacting on the Venmo Platform.

30. Plaintiff Rundzio used the Venmo Platform intermittently, and he was intent on keeping his transactions private. Because he purposefully selected the private setting each time he sent money, Plaintiff Rundzio had an expectation of privacy in each transaction and felt comfortable including full and accurate descriptions of what his payments were for—even writing his daughter's name and identifying the establishment where she participated in extracurricular activities—to denote how, to whom, and for what purpose a payment was allocated. Like other Class Members, Plaintiff Rundzio was not clearly and conspicuously informed that even setting each transaction to private would not prevent his information from being shared with third parties.

31. Unbeknownst to Plaintiff Rundzio, PayPal disclosed, and the Third-Party Recipients intercepted and recorded, Plaintiff Rundzio's PII, which includes transaction information such as recipient details and notes associated with each transaction.

32. Plaintiff Nathan Olson ("Plaintiff Olson") is a citizen and resident of Garden Grove, California.

33. Plaintiff Olson has a Venmo account.

34. Plaintiff Olson used the Venmo Platform mobile application on his personal iPhone device to send and receive monetary payments for personal reasons.

35. To open and use a Venmo account, Plaintiff Olson was required to provide PayPal with his full name, email address, telephone number, and financial banking account information.

36. Plaintiff Olson's Venmo account and/or individual transactions were set to "Private," meaning that, according to PayPal's own representations, PayPal would "not share the transaction

anywhere other than in your personal transactions feed under the Me tab and with the other participant."[12]

37. Plaintiff Olson read and relied on PayPal's representations regarding the privacy and security of the Venmo Platform, including Venmo's in-application privacy settings and Venmo's marketing representations that transactions are encrypted and secure, before providing Plaintiff Olson's information to PayPal and before transacting on the Venmo Platform.

38. Plaintiff Olson used the Venmo Platform frequently, and he sent the majority of his transactions with the expectation that they would remain private. Because he had an expectation of privacy with his account set to private, Plaintiff Olson felt comfortable using his Venmo account as he saw fit. Like other Class Members, Plaintiff Olson was not clearly and conspicuously informed that even setting his account to private would not prevent his information from being shared with third parties.

39. Unbeknownst to Plaintiff Olson, PayPal disclosed, and the Third-Party Recipients intercepted and recorded, Plaintiff Olson's PII, which includes transaction information such as recipient details and notes associated with each transaction.

40. Plaintiffs did not consent to the disclosure or interception of this data, or to its use by PayPal or the Third-Party Recipients.

41. Plaintiffs continue to face an ongoing risk of injury. Plaintiffs cannot determine whether PayPal has ceased the conduct alleged herein, and the data already disclosed remains in the possession of the Third-Party Recipients and has not been destroyed.

42. The option to simply "close an account" ignores the reality that many users of the Venmo Platform rely on the platform for both personal and professional purposes and frequently maintain funds in their Venmo accounts. Closing an account is therefore far more onerous than

[12] Help Center, Manage your Venmo privacy settings, Venmo, https://help.venmo.com/cs/articles/manage-your-venmo-privacy-settings-vhel351 (last visited August 26, 2026).

Defendant suggests, underscoring that users never had a meaningful opportunity to reject the New User Agreement.

43. Plaintiff Lana Nava ("Plaintiff Nava") is a citizen and resident of Brisbane, California.

44. Plaintiff Nava has a Venmo account.

45. Plaintiff Nava used both the Venmo Platform mobile application on her personal iPhone device and the Venmo Platform website to send and receive monetary payments for personal and work-related reasons.

46. Plaintiff Nava also has the Venmo-branded debit card, which she frequently uses to make personal transactions. Plaintiff Nava also receives her payroll through Venmo.

47. To open and use a Venmo account, Plaintiff Nava was required to provide the Venmo Platform with her full name, email address, telephone number, and financial banking account information.

48. Plaintiff Nava's Venmo account and/or individual transactions were set to "Private," meaning that, according to PayPal's own representations, PayPal would "not share the transaction anywhere other than in your personal transactions feed under the Me tab and with the other participant."[13]

49. Plaintiff Nava read and relied on PayPal's representations regarding the privacy and security of the Venmo Platform, including Venmo's in-application privacy settings and Venmo's marketing representations that transactions are encrypted and secure, before providing Plaintiff Nava's information to PayPal and before transacting on the Venmo Platform.

50. Plaintiff Nava used the Venmo Platform extensively, and many of her monetary transactions took place on the Venmo Platform. Plaintiff Nava had an expectation of privacy with her account set to private. Like other Class Members, Plaintiff Nava was not clearly and

---

[13] Help Center, Manage your Venmo privacy settings, Venmo, https://help.venmo.com/cs/articles/manage-your-venmo-privacy-settings-vhel351 (last visited August 26, 2026).

conspicuously informed that even setting her account to private would not prevent her information from being shared with third parties.

51. Unbeknownst to Plaintiff Nava, PayPal disclosed, and the Third-Party Recipients intercepted and recorded, Plaintiff Nava's PII, which includes transaction information such as recipient details and notes associated with each transaction.

B. Defendant

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

53. PayPal owns and operates the Venmo Platform, including the Venmo website located at www.venmo.com and the Venmo mobile applications distributed through the Apple App Store and the Google Play Store. PayPal drafts and publishes the Venmo User Agreement, the Venmo Privacy Statement, and the Venmo Help Center materials described herein.

54. PayPal knowingly and intentionally incorporated the Tracking Technology into the Venmo Platform. PayPal exercised complete control over that technology, including which screens and user actions it monitored, which data fields it transmitted, how transmitted events were named and configured, and which third parties received them.

55. PayPal knew at the time it incorporated this technology that doing so would result in the disclosure to, and interception by, third parties of Plaintiffs' and Class Members' PII, by virtue of how the technology functions and the analytics, attribution reporting, and marketing capabilities PayPal received in return.

JURISDICTION AND VENUE

56. This Court has subject matter jurisdiction under 28 U.S.C. § 1332(d) because the amount in controversy for the Class exceeds $5,000,000, exclusive of interest and costs, there are more than 100 members of the proposed Classes, and a significant portion of the members of the proposed Classes are citizens of states different from Defendant.

57. This Court also has federal-question jurisdiction under 28 U.S.C. § 1331 because Plaintiffs assert claims arising under the laws of the United States, namely, the Electronic Communications Privacy Act, 18 U.S.C. §§ 2510 *et seq.*

58. This Court has supplemental jurisdiction over the state-law claims under 28 U.S.C. § 1367 because those claims are so related to the federal claim that they form part of the same case or controversy under Article III of the United States Constitution.

59. This Court has personal jurisdiction over PayPal because its principal place of business is in California and a substantial part of the events and conduct giving rise to Plaintiffs' claims occurred in this State, including the design, configuration, and deployment of the Tracking Technology, the disclosure of Plaintiffs' and Class Members' data, and the use of that data for commercial purposes.

60. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b), (c), and (d) because PayPal is headquartered in this District, is subject to personal jurisdiction in this District, and a substantial part of the events and omissions giving rise to Plaintiffs' claims occurred in this District.

61. **Divisional Assignment:** This action arises in Santa Clara County, in that a substantial part of the events that give rise to the claims asserted herein occurred in Santa Clara County. Pursuant to Civil L.R. 3-2(e), all civil actions that arise in Santa Clara County shall be assigned to the San Jose Division.

62. PayPal's use of the Tracking Technology began long before the New User Agreement[14] went into effect.

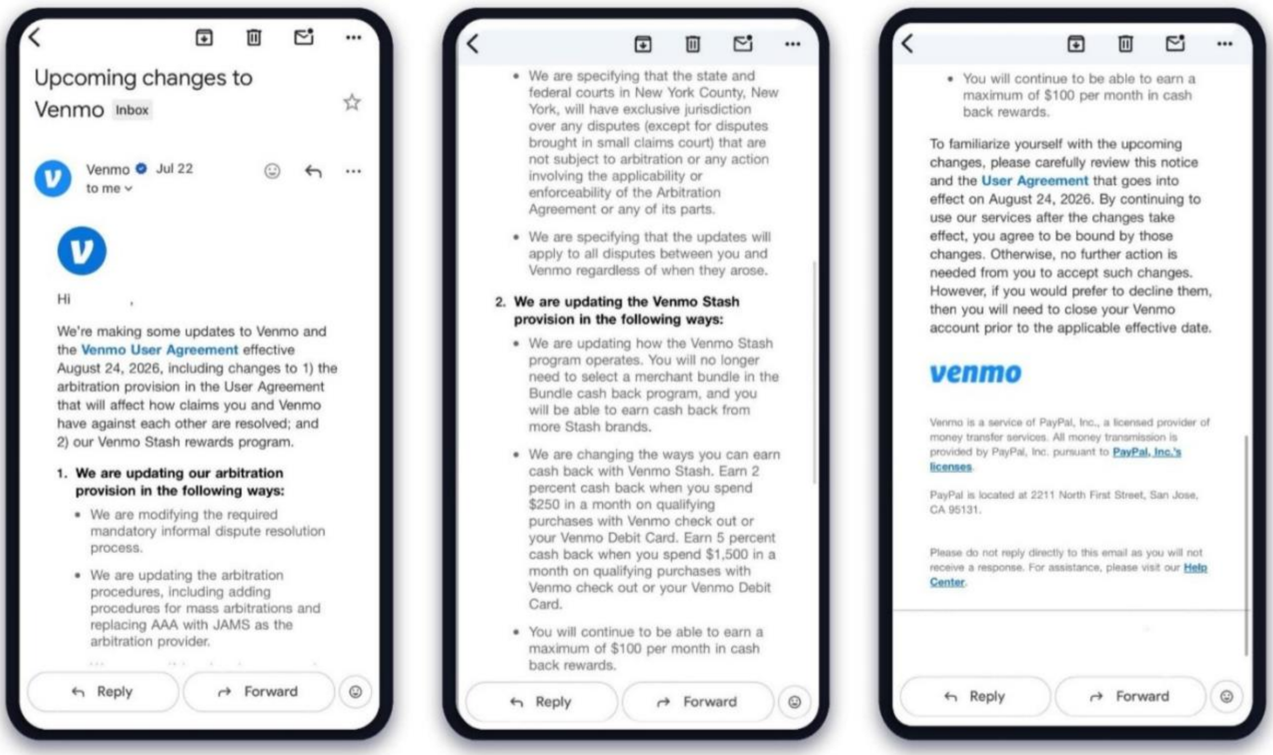
63. Defendant's operative User Agreement provides that all disputes against Defendant shall be brought in arbitration. However, because the arbitration clause is unconscionable and unenforceable, this case is properly brought in this Court.

---

[14] Venmo User Agreement (DATE EFFECTIVE: August 24, 2026) (the "New User Agreement") (*See* Exhibit B attached to the Complaint).

64. On or around July 22, 2026, PayPal emailed its users notifying them of substantial changes to the New User Agreement, which included updates to the arbitration clause and the "Venmo Stash" provision,[15] effective August 24, 2026, as reflected in **Figure 1** below:

Figure 1



65. The New User Agreement did not merely modify the Former User Agreement[16]—it strategically removed the core consumer protections that had made individual and mass arbitration a viable path to relief, stripping away rights users held as recently as August 23, 2026.[17]

66. As described in detail below, the changes were not incidental adjustments to routine business terms; they were specifically and precisely engineered to defeat noticed claims, and to

[15] *Id.*

[16] Venmo User Agreement (DATE EFFECTIVE: May 19, 2026) (the "Former User Agreement") (*See* Exhibit C attached to the Complaint).

[17] New User Agreement.

make mass arbitration functionally impossible going forward—forcing consumers instead into costly, isolated, individual proceedings that few could afford to pursue. Individually and in combination, these changes are so one-sided, so clearly designed to unnecessarily complicate the PayPal mass-arbitration process, and so contrary to the very purpose of a dispute-resolution process, that they render the New User Agreement's arbitration provisions unconscionable and unenforceable. Specifically:

A. Where the Former User Agreement required only written notice to initiate the informal dispute resolution process, the New User Agreement now requires that any Notice of Dispute bear an <u>*original handwritten signature*</u>—a formality with no purpose other than to create an additional procedural hurdle for claimants proceeding at scale.[18]

B. The Former User Agreement's informal dispute resolution period was 45 days. The New User Agreement expands that period to 60 days, and longer still if PayPal elects to request a conference—unreasonably extending, at PayPal's unilateral option, the minimum time every claimant must wait before they may even file for arbitration.[19]

C. A represented claimant must now separately execute a <u>*signed handwritten authorization*</u> before that claimant's own counsel may discuss the dispute or review the claimant's account records with PayPal. The Former User Agreement includes no such requirement. This new requirement serves as yet another procedural hurdle serving no purpose but PayPal's own benefit, which claimants alone are forced to clear.[20]

---

[18] *Id.* § Mandatory Informal Dispute Resolution Process.

[19] *Id.*

[20] *Id.*

D. Per the New User Agreement, where 25 or more similar disputes are asserted by the same or coordinated counsel, only 25 claims selected by each side (50 total) will proceed as filed arbitration cases at any one time, and no fees will be assessed for, and no other case will be administered among, the remaining claims until the pending cases are resolved. The Former User Agreement contained no mechanism limiting how many claims could proceed to arbitration at once. For claimants represented by counsel handling a meaningful volume of similar disputes, this provision does not merely delay relief—it forecloses it, potentially for years.[21]

E. The Former User Agreement expressly provided that any future amendment "shall not apply to any claim that was filed in a legal proceeding against PayPal or you prior to the effective date of the amendment."[22] The New User Agreement now does precisely what that provision promised PayPal would not do: it declares that it applies "notwithstanding any provision in any prior Agreement to Arbitrate to the contrary" and governs "all Disputes, including all Disputes that arose before the effective date of th[e] Arbitration Agreement."[23] This reversal is not incidental—it is a direct repudiation of a promise PayPal itself made in writing, precisely the kind of one-sided, after-the-fact rewriting of a bargained-for term that renders a contract provision substantively unconscionable by allowing PayPal to abandon its own written commitments whenever doing so serves its interests, while consumers remain bound to arbitrate on whatever terms PayPal unilaterally decides to impose on that day.

---

[21] *Id.* § Additional Procedures for Mass Arbitration.

[22] Former User Agreement § Future Amendments to this Agreement to Arbitrate.

[23] New User Agreement § Superseding Arbitration Agreement.

F. Existing users are not permitted to opt out of these amended terms: the sole opt-out mechanism identified in the amended terms is available only to a user who provides written notice within 30 days of that user's first acceptance of any Venmo user agreement. PayPal offers no other means by which an existing user may decline the amended terms other than closing the user's Venmo account entirely.[24]

G. The Former User Agreement contained no provision purporting to seize disputes already pending in another arbitral forum. The New User Agreement does exactly that, mid-dispute and without consent—providing that any filed or pending arbitration must be subject to the new arbitration agreement and forum even where that dispute is, at that very moment, already pending before a different arbitration provider.[25]

H. The Former User Agreement required no advance certification before a claimant could file for arbitration. The New User Agreement now requires that a certification of compliance be mailed before filing with an arbitration forum—one more procedural checkpoint interposed between a consumer and relief.[26]

67. Critically, the New User Agreement also eliminates the single most important protection for consumers with modest claims. The Former User Agreement committed, without qualification, that PayPal would pay all arbitration fees for claims of $10,000 or less.[27] The New User Agreement replaces that commitment with the following language: PayPal and the user "may elect to engage with [the arbitration provider] regarding the reduction or deferral of arbitration fees,"

[24] *Id.* § Opt-Out Procedure.

[25] *Id.* § Superseding Arbitration Agreement.

[26] *Id.* § Arbitration Procedures.

[27] Former User Agreement.

and the parties "will work together in good faith to ensure that arbitration remains cost-effective."[28] A promise to pay became a promise to talk.

68. Considered individually, each of these changes disadvantages consumers. Considered together, they demonstrate a coordinated redesign of the dispute resolution process, adopted in the span of a single email most users will never see or read, that so materially increases the burden to pursue arbitration in both an individual and mass arbitration it becomes procedurally unworkable and prohibitively expensive for individual consumers.

69. PayPal's July 22, 2026 email to users indicated that if they did not want to be subject to the new terms then a user "will need to close your Venmo account prior to the applicable effective date." However, the process for closing one's Venmo account is complex. Indeed, many users tried and failed to do so by the deadline. To close one's account one must: "move any money remaining in your Venmo account before closing it," and wait for "any pending transactions on Venmo."[29] Once it is confirmed that no other transactions are pending, one must "[g]o to the "Me" tab by tapping your picture or initials," then "Tap the Settings gear," then "Select Account under Preferences," then click "Close Venmo Account."[30]

70. The arbitration clause contained in the New User Agreement is unconscionable and unenforceable, and thus this case is properly brought in this Court for several reasons, including the following:

71. First, because the New User Agreement contains a mass-arbitration protocol—including batching of claims, use of bellwethers, and delayed/staged filings—the arbitration agreement is unenforceable under *Heckman v. Live Nation Entertainment, Inc.*, 120 F.4th 670 (9th Cir. 2024), and *Discover Bank v. Superior Court*, 36 Cal.4th 148, 30 Cal.Rptr.3d 76 (2005). Mass

---

[28] New User Agreement § Costs of Arbitration.

[29] How can we help you? Close My Venmo Account, Venmo, https://help.venmo.com/cs/articles/close-my-venmo-account-vhel267 (last visited August 28, 2026).

[30] *Id.*

arbitration protocols do not involve bilateral arbitration proceedings and are therefore not subject to any Federal Arbitration Act ("FAA") provision that preempts California's *Discover Bank* rule prohibiting the waiver of class actions through arbitration agreements. This means *Discover Bank*'s unconscionability test applies to the class-action waiver here, notwithstanding the arbitration clause. Applying that test, the waiver is unconscionable and unenforceable.

72. Second, the staged bellwether process ties the timing of a claimant's case not to the merits of that claim, but to how many other similarly situated claimants happen to be represented by that claimant's own counsel. This is specifically designed to prejudice claimants who retain a mass arbitration firm. Because only a limited number of cases may proceed to filing at any one time, a claimant represented by counsel who represents many similarly situated clients—typically the most experienced and qualified counsel available for this type of claim—may be forced to wait years, if not more, before their individual claim is even filed. A claimant represented by counsel with few or no other similar clients faces no comparable bottleneck and may proceed to filing immediately, regardless of that counsel's relative experience or qualifications. *See Pandolfi v. AviaGames, Inc.*, No. 23-CV-05971-EMC, 2024 WL 4051754 (N.D. Cal. Sept. 4, 2024). The practical effect is to penalize claimants for retaining experienced counsel who represent multiple similarly situated clients, and to pressure those claimants into abandoning their counsel and/or proceeding alone to avoid the staged process's delay. This is itself independently unconscionable: it conditions how quickly a consumer may vindicate their rights on nothing more than the caseload of the lawyer that consumer chose to hire.

73. Third, the staged bellwether provision in the New User Agreement is further unconscionable as it functions as a prospective waiver of users' rights to pursue statutory remedies—including remedies for privacy violations under federal and state law. The New User Agreement's staged bellwether provision prevents Plaintiffs and Class Members from even filing their claims in arbitration for potentially many years—and realistically, indefinitely—based solely on the identity of their chosen legal counsel. Plaintiffs and the Classes are therefore unable to

exercise their rights to pursue important statutory remedies available to them for the harm caused by PayPal.

74. Fourth, the staged bellwether provision is further procedurally unconscionable because it constitutes procedural surprise. Even if Plaintiffs had the opportunity to read and understand the User Agreement, the fact that they must wait an indiscernible number of years to even file their claims in the arbitration forum is a procedural surprise. Plaintiffs and Class Members also lack the ability to know the identity of their counsel, their counsel's other clients, and the nature of those other clients' claims so as to be able to anticipate having their individual claims delayed or suspended indefinitely by having similar claims.

75. Fifth, the New User Agreement is procedurally unconscionable as it is an adhesion contract between parties of unequal relative bargaining positions (large corporation vs. individual consumer), and presented in a complex, 76-page mostly single-spaced document,[31] and written in dense legalese that is difficult for ordinary laypersons to understand.

76. Sixth, there is no notice to Class Members in the New User Agreement that Defendant and third parties engage in the privacy practices challenged below so they would be aware of the need to review the User Agreement. PayPal's failure to disclose this information was an omission of material fact to Plaintiffs and other reasonable consumers in the class. The arbitration clause in the New User Agreement is designed to delay the initiation and adjudication of claims and to create a process aimed at discouraging consumers from vindicating their rights.

77. For these and other reasons, PayPal's arbitration provision in the New User Agreement is unenforceable, and Plaintiffs' and Class Members' claims are properly brought in this Court.

78. PayPal's conduct violated the Electronic Communications Privacy Act, 18 U.S.C. §§ 2510 *et seq.* ("ECPA"); the California Invasion of Privacy Act, Cal. Penal Code §§ 630 *et seq.*

[31] The New User Agreement when converted to PDF format from its online version becomes an approximately 76-page mostly single-spaced document.

("CIPA"); the California Comprehensive Computer Data Access and Fraud Act, Cal. Penal Code § 502 ("CDAFA"); Article I, Section 1 of the California Constitution; the California Unfair Competition Law, Cal. Bus. & Prof. Code §§ 17200 *et seq.* ("UCL"); and the common law, including invasion of privacy, unjust enrichment, and negligence.

79. Given the secret and undisclosed nature of PayPal's conduct, additional evidence supporting Plaintiffs' claims—including the full universe of third parties that received Venmo user data, the full set of data fields transmitted, and how that data was used—is uniquely within PayPal's possession and will be revealed in discovery.

FACTUAL BACKGROUND

A. The Venmo Platform and the Sensitivity of Venmo Transaction Data

80. Venmo is a peer-to-peer payment platform. Users link a bank account, debit card, or credit card to a Venmo account and use the Venmo Platform to send money to, and request money from, other individuals and businesses. Some users have a Venmo debit card that they use for banking purposes.

81. To create a Venmo account, a user must provide PayPal with, at minimum, their full legal name, email address, telephone number, and financial account information, and must verify their identity.

82. Each Venmo payment consists of several discrete pieces of information supplied by the user: the identity of the counterparty, the dollar amount, and a text "note" field. The note field is mandatory when an account is set to private; a Venmo user cannot complete a payment without entering a description of what the payment is for.

83. Because the note field is required, and because the Venmo Platform is used for the most routine and the most personal transactions alike, Venmo transaction records are extraordinarily revealing. In the aggregate and often individually, they disclose where a person lives and with whom, what medical and mental-health providers they see, what medications and treatments they pay for, whether they are in addiction recovery, whether they are struggling to make rent, whom

they date, what political candidates and religious institutions they support, what attorneys they retain, and what they buy.

84. For example, Plaintiff Rundzio sent transactions to parties describing a payment made for a class his daughter took. This payment had a detailed description that included his daughter's name, the class she took, and the date on which the class occurred.

85. Financial transaction data of this kind has long been recognized as deserving of heightened protection. Congress enacted the GLBA, 15 U.S.C. §§ 6801 *et seq.* to require financial institutions to protect the security and confidentiality of customers' nonpublic personal information. Similarly, California enacted the California Financial Information Privacy Act, Cal. Fin. Code §§ 4050 *et seq.* ("CFIPA"), to impose stricter limits on the sharing of consumer financial information than federal law requires.

86. PayPal is a financial institution subject to these regimes, and it holds itself out to consumers as such. The Venmo Privacy Statement is presented in the format prescribed for GLBA privacy notices, including the standardized table captioned: "Reasons we can share your personal information", "Does Venmo share?" and "Can you limit this sharing?"[32]

B. PayPal's Privacy Promises to Venmo Users

87. PayPal has made express and implied representations to Venmo users, across multiple channels, that their PII, which includes transaction information such as recipient details and notes associated with each transaction, would not be disclosed to third parties.

88. The Venmo Privacy Statement expressly represents: "Venmo does not disclose your personal information with third parties for their promotional or marketing purposes."[33]

89. The Venmo Privacy Statement states that, as to sharing "[f]or nonaffiliates to market to you," PayPal does not share, and that the consumer need not limit such sharing because "[w]e

---

[32] Venmo Privacy Statement.

[33] *Id.*

don't share."[34] The Venmo Privacy Statement defines "Nonaffiliates" as "[c]ompanies not related by common ownership or control," which "can be financial and nonfinancial companies."[35] mParticle and Kochava are nonaffiliates within this definition.

90. The Venmo Privacy Statement further represents that only "[s]ome personal information"—that which "is public information and may be seen by anyone on the internet, whether or not they have a Venmo account"—"may also be seen, accessed, reshared or downloaded through Venmo's APIs or third-party services that integrate with our products."[36]

91. The Venmo Privacy Statement defines that narrow category: "Public information ... includes your Venmo username, profile photo, first and last name, month and year of Venmo account creation, and public transactions in which you've been involved."[37] It does not include private transactions, transaction amounts, transaction notes, email addresses, telephone numbers, or device and advertising identifiers.

92. The Venmo Privacy Statement also tells users they control what is shared: "In addition to any public information, your Venmo friends list may be seen by any logged-in Venmo user; you may adjust or turn off this setting in the privacy section in your account settings."[38]

93. The Venmo Privacy Statement makes a specific promise to California users: "If your Venmo account has a California mailing address, we will not share personal information we collect about you except to the extent permitted under California law."[39]

---

[34] *Id.*

[35] *Id.*

[36] *Id.*

[37] *Id.*

[38] *Id.*

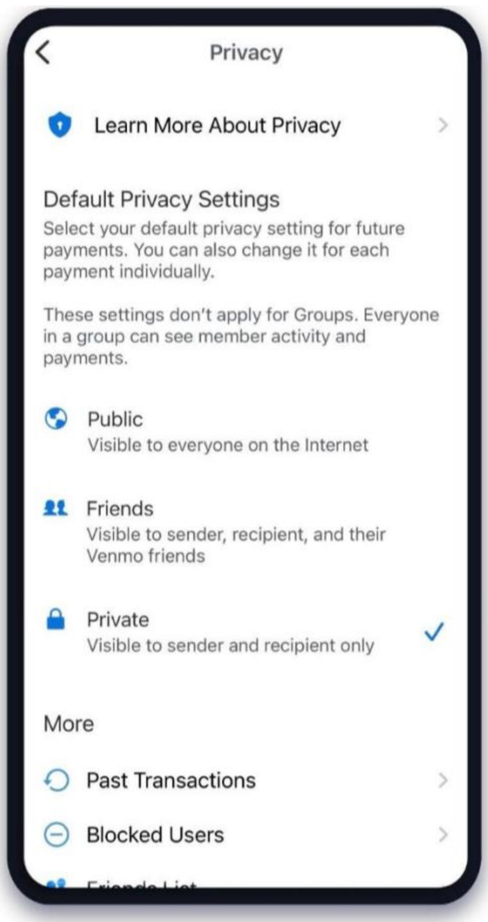
[39] *Id.*

94. The Venmo Privacy Statement is not limited to any particular context. It states expressly: "This Privacy Statement applies to all information we collect through our Services from current and former Venmo users."[40]

95. ***The Venmo Privacy Settings and Help Center.*** PayPal offers Venmo users three privacy settings for their payments and explains each in the Venmo Platform mobile app and Venmo Help Center, which is prominently linked from the Venmo website.

As reflected in **<u>Figure 2</u>** below, there are three privacy options available for users' payments:[41]

<u>Figure 2</u>



---

[40] *Id.*

[41] Help Center, Manage your Venmo privacy settings, Venmo, https://help.venmo.com/cs/articles/manage-your-venmo-privacy-settings-vhel351 (last visited August 26, 2026).

96. PayPal's representation that a "Private" transaction will not be shared "anywhere other than in your personal transactions feed under the Me tab and with the other participant" is unqualified.[42] It contains no carve-out for analytics providers, such as the Third-Party Recipients, marketing partners, attribution vendors, customer data platforms, or any other third party.

97. PayPal further assures users that PayPal safeguards their data: "We use encryption to help protect your account details and store that information on servers in secure locations. On the web, 'https:' and a lock icon next to the web address is your signal that encryption is on."[43]

98. ***Venmo's Marketing Representations.*** PayPal repeated and amplified these promises in its consumer-facing marketing. On the page describing the Venmo Platform's approach to "Trust & Safety," PayPal told consumers: "Send dollars, not financial details . . . Every transaction in our app is encrypted, so your financial information stays secure whether you're paying a friend or checking out online."[44]

99. PayPal likewise promised users "[s]ecure transactions" on the page through which consumers are directed to begin using the Venmo Platform.[45]

100. Taken together, these representations assured Plaintiffs and Class Members that PayPal would not disclose their PII to anyone other than the counterparty to the transaction, in any context.

C. PayPal Disclosed Venmo Users' PII to Third Parties

101. Contrary to these representations, PayPal purposefully embedded the Tracking Technology on the Venmo Platform that caused Plaintiffs' and Class Members' PII, which includes

---

[42] *Id.*

[43] About Venmo Security, Venmo, https://help.venmo.com/cs/articles/about-venmo-security-vhel224 (last visited August 26, 2026).

[44] Trust & Safety, A safe way to pay and get paid, Venmo, https://venmo.com/about/us/trust-and-safety (last visited August 26, 2026).

[45] Got paid for dinner? Turn it into dessert when you pay with Venmo, Venmo, https://venmo.com/pay/start (last visited August 26, 2026).

transaction information such as recipient details and notes associated with each transaction, to be transmitted to and intercepted and recorded by third parties, including mParticle and Kochava.

102. Through this Tracking Technology, PayPal caused the unauthorized interception and disclosure of each of the following data fields: the sender's full name; AAID; email address; phone number; mParticle ID; Kochava ID; the identity of the recipient of the transaction; the amount paid; and the note describing the purpose of the transaction.

103. These transmissions occurred contemporaneously with the user's communication of the payment instruction to PayPal—that is, while the communication was in transit to its intended recipient, PayPal, and before it reached PayPal's servers.

104. The transmissions occurred regardless of the privacy setting the user had selected. A user who marked a transaction "Private," and who therefore had been told by PayPal that the transaction would not be shared "anywhere other than in your personal transactions feed under the Me tab and with the other participant," nonetheless had that transaction's counterparty, amount, and note disclosed to third parties.[46]

105. PayPal received a direct commercial benefit from these disclosures, including analytics regarding user behavior, attribution reporting that allowed PayPal to measure the effectiveness of its paid advertising, the ability to construct and target custom audiences, and the ability to route user data to additional downstream marketing and advertising partners.

D. mParticle's Tracking Technology on the Venmo Platform

106. mParticle is a customer data platform, or "CDP." Its business consists of ingesting user-level data from its customers' websites and mobile applications, unifying that data into a persistent profile for each individual, and routing that profile and the underlying event data to downstream partners including advertising networks, analytics providers, marketing automation vendors, and data warehouses.

---

[46] Help Center, Manage your Venmo privacy settings, Venmo, https://help.venmo.com/cs/articles/manage-your-venmo-privacy-settings-vhel351 (last visited August 26, 2026).

107. To accomplish this, mParticle assigns each individual a unique and persistent identifier, the mParticle ID, which functions as the key linking every event, device, and identifier associated with that person. mParticle expressly encourages its customers to transmit directly identifying information, including names, email addresses, and telephone numbers, so that individuals can be resolved to a single profile across applications and devices.

108. PayPal incorporated mParticle's Tracking Technology into the Venmo Platform. As a result, PayPal disclosed, and mParticle intercepted, Plaintiffs' and Class Members' full names, email addresses, telephone numbers, AAIDs, mParticle IDs, and the counterparty, amount, and note associated with their Venmo transactions.

109. mParticle is not a party to Plaintiffs' or Class Members' communications with PayPal. Plaintiffs and Class Members did not know mParticle existed, did not know mParticle's code was executing on their devices, and did not consent to mParticle's receipt of their private financial transaction data.

110. Upon information and belief, mParticle used the data it received from the Venmo Platform for its own commercial purposes, including to improve its identity-resolution capabilities and its products and services, and routed that data onward to additional third parties at PayPal's direction. The full set of downstream recipients is within PayPal's exclusive knowledge and will be identified in discovery.

E. Kochava's Tracking Technology on the Venmo Platform

111. Kochava is a mobile measurement and attribution company. Its core product allows application developers to determine which advertisements caused a given individual to install and use their application, which necessarily requires Kochava to identify and track specific individuals across applications and over time.

112. Kochava assigns each individual a unique and persistent identifier—the Kochava ID—and links that identifier to device-level identifiers such as the AAID, as well as to directly identifying information supplied by its customers.

113. Kochava also operates as a data broker. The Federal Trade Commission previously sued Kochava in connection with its collection and sale of sensitive consumer data and settled with the company in May 2026. *See Federal Trade Commission v. Kochava Inc.*, 671 F.Supp.3d 1161 (2023).

114. PayPal incorporated Kochava's Tracking Technology into the Venmo Platform. As a result, PayPal disclosed, and Kochava intercepted, Plaintiffs' and Class Members' PII, including their Kochava IDs and AAIDs.

115. Kochava is not a party to Plaintiffs' or Class Members' communications with PayPal, and Plaintiffs and Class Members did not consent to Kochava's receipt of their data.

F. The Disclosed Data Uniquely Identified Each Class Member

116. The information PayPal disclosed was not aggregated, deidentified, hashed, or anonymized in any manner that would prevent the Third-Party Recipients from identifying the specific individual to whom it pertained.

117. To the contrary, PayPal transmitted directly identifying information—full name, email address, and telephone number—in the same transmissions as the transaction data.

118. PayPal also transmitted persistent unique identifiers, including the AAID, mParticle ID, and Kochava ID. These identifiers exist for the sole purpose of singling out one specific individual and following that individual across applications, websites, and devices over time. They function much like a Social Security number: each is associated with exactly one person, and the entity that assigns it knows which person that is.

119. The AAID in particular is a device-resident advertising identifier that is available to every application on an Android device and is widely used across the advertising industry as a common key for joining data about a person collected from otherwise unrelated sources.

120. Accordingly, the Third-Party Recipients could and did associate the Venmo transaction data they received with an identified individual and with the other data they already maintained about that individual.

G. Plaintiffs and Class Members Did Not Consent

121. Plaintiffs and Class Members had no way of knowing that PayPal was disclosing, and the Third-Party Recipients were intercepting, their PII, which includes transaction information such as recipient details and notes associated with each transaction, because the Tracking Technology is incorporated invisibly in the background of the Venmo Platform.

122. Nothing in the Venmo User Agreement, the Venmo Privacy Statement, the Venmo Help Center, the Venmo website, or the Venmo Platform itself disclosed that private transaction details—counterparty, amount, and note—would be transmitted to third-party data companies, such as the Third-Party Recipients.

123. To the contrary, PayPal's disclosures affirmatively represented the opposite: that only "public information"[47] would be accessible through "third-party services that integrate with our products," and that "Private" transactions would not be shared "anywhere other than in your personal transactions feed under the Me tab and with the other participant."[48]

124. Consent is effective only where the defendant has made disclosures that explicitly notify the user of the particular conduct, or substantially the same conduct, and the defendant has not exceeded the scope of that consent. Where a privacy notice makes specific representations that could suggest to a reasonable user that a party would not engage in the alleged data collection, there is no consent.

125. PayPal's representations here go well beyond ambiguity. They are affirmative promises that the precise conduct at issue would not occur.

126. PayPal also may not rely on any purported consent obtained through the Venmo privacy settings. Those settings are the very mechanism by which PayPal represented that

---

[47] Venmo Privacy Statement.

[48] Help Center, Manage your Venmo privacy settings, Venmo, https://help.venmo.com/cs/articles/manage-your-venmo-privacy-settings-vhel351 (last visited August 26, 2026).

transactions would be kept private. A user who selected "Private" expressly withheld consent to any sharing beyond the counterparty.

H. Plaintiffs and Class Members Have a Reasonable Expectation of Privacy in Their Transaction Data

127. Plaintiffs and Class Members have a reasonable expectation of privacy in their communications on the Venmo Platform, including the identity of their counterparties, the amounts they paid, the notes describing their transactions, and the PII associated with their accounts.

128. This is especially true when Plaintiffs and Class Members specifically set their Venmo Platform settings to "Private."

129. That expectation is reinforced by longstanding social and legal norms treating an individual's financial records as private, and by the federal and state statutory schemes—including the GLBA and the California Financial Information Privacy Act—that restrict financial institutions' sharing of consumer financial information.

130. It is further reinforced by PayPal's own conduct in building a per-transaction privacy control into the Venmo Platform, and by PayPal's express representations about what that control does.

131. Privacy polls and studies uniformly show that the overwhelming majority of Americans consider affirmative consent before a company collects and shares personal data to be among the most important privacy protections. A study by Consumer Reports found that 92% of Americans believe internet companies and websites should be required to obtain consent before selling or sharing consumers' data.[49] According to Pew Research Center, approximately 81% of Americans are concerned about how companies collect data about them.[50]

---

[49] Consumer Reports Survey Group, *Social Media & Privacy Survey* (Jan. 2018).

[50] Colleen McClain, Michelle Faverio, Monica Anderson & Eugenie Park, *How Americans View Data Privacy: The Role of Technology Companies, AI and Regulation*, Pew Research Center (Oct. 18, 2023).

132. PayPal’s surreptitious disclosure of Plaintiffs’ and Class Members’ PII, which includes transaction information such as recipient details and notes associated with each transaction, in direct contradiction of its own promises, violates those expectations and would be highly offensive to a reasonable person.

133. Further, once PayPal transmits a user’s PII, which includes transaction information such as recipient details and notes associated with each transaction, to the Third-Party Recipients, PayPal has no control over what those Third-Party Recipients do with that data, whom they further disclose it to, or how it is ultimately used. PayPal therefore cannot credibly represent that any resulting risk to Plaintiffs’ and Class Members’ privacy is remote or speculative—by PayPal’s own design, PayPal itself has no way of knowing who ultimately possesses the data or what they intend to do with it.

I. The Disclosed Data Has Substantial Economic Value

134. The data PayPal disclosed is valuable, and PayPal disclosed it precisely because it is valuable.

135. Financial transaction data—what a person buys, from whom, how often, and for how much—is among the most sought-after categories of data in the advertising and marketing industries, because it reflects actual behavior rather than inferred intent.

136. An entire industry exists to acquire, enrich, and resell consumer data of this kind. Data brokers and customer data platforms generate substantial revenue by aggregating individual-level data from many sources and monetizing the resulting profiles.

137. Consumers likewise place value on this data. Plaintiffs and Class Members would not share sensitive personal data with a digital platform for free, and many would abandon brands that fail to protect their data. Viewed in isolation, the disclosure of one person’s data might seem troubling but not necessarily egregious. Consider the sheer size of Venmo’s user base, tens of millions of users, the volume of transactions each user makes, and the fact that every one of those transactions was transmitted to third parties to build profiles of those users—the true scale and

severity of PayPal's conduct comes into focus. This data alone forms a nearly complete picture of a person.

138. PayPal received value in exchange for the data it disclosed, in the form of analytics, attribution reporting, audience-building capabilities, and improved advertising performance. Plaintiffs and Class Members received nothing.

TOLLING, CONCEALMENT, AND ESTOPPEL

139. The applicable statutes of limitations have been tolled as a result of PayPal's knowing and active concealment and denial of the facts alleged herein.

140. PayPal secretly incorporated the Third-Party Recipients' Tracking Technology into the Venmo Platform, providing no indication to users that their PII and transaction information were being shared with third parties.

141. PayPal had exclusive knowledge that the Venmo Platform incorporated this Tracking Technology and failed to disclose that fact to users. To the contrary, PayPal affirmatively represented that private transactions would not be shared beyond the counterparty.

142. Plaintiffs and Class Members could not, even with due diligence, have discovered PayPal's conduct. The conduct is highly technical, occurs invisibly within compiled mobile application code and server-side transmissions, and was contradicted by every disclosure PayPal made.

143. PayPal was under a duty to disclose the nature and significance of its data-sharing practices and did not do so. PayPal is therefore estopped from relying on any statute of limitations, and the discovery rule and the doctrine of fraudulent concealment toll all applicable limitations periods.

CLASS ACTION ALLEGATIONS

144. Plaintiffs bring this action pursuant to Federal Rule of Civil Procedure 23 individually and on behalf of the following Class:

> **Nationwide Class:** All natural persons in the United States who (i) used the Venmo Platform; (ii) had their privacy settings set to private

> or enabled at least one transaction set to private; (iii) whose PII was disclosed to, transmitted to, made accessible to, or intercepted by third parties; and (iv) who have not filed a demand for arbitration against PayPal relating to the above misconduct.

145. In addition or in the alternative, Plaintiffs plead the following California Subclass:

> **California Subclass:** All natural persons residing in California who (i) used the Venmo Platform; (ii) had their privacy settings set to private or enabled at least one transaction set to private; (iii) whose PII was disclosed to, transmitted to, made accessible to, or intercepted by third parties; and (iv) who have not filed a demand for arbitration against PayPal relating to the above misconduct.

146. Excluded from the Class and Subclass are: (1) any Judge or Magistrate Judge presiding over this action and any members of their immediate families; (2) PayPal, its subsidiaries, affiliates, parents, successors, and predecessors, any entity in which PayPal or its parents have a controlling interest, and their current or former employees, officers, and directors; and (3) Plaintiffs' counsel and PayPal's counsel.

147. ***Numerosity.*** The exact number of members of the Class and Subclass is unknown and unavailable to Plaintiffs at this time, but individual joinder is impracticable. The Class and Subclass likely consist of millions of individuals, each of whom can be identified through PayPal's records.

148. ***Predominant Common Questions.*** Common questions of law and fact predominate over any questions affecting only individual members, and include, but are not limited to:

A. Whether PayPal incorporated the Tracking Technology into the Venmo Platform;

B. Whether PayPal disclosed, and third parties intercepted and recorded, Class Members' PII;

C. Which data fields were disclosed, and to which third parties;

D. Whether PayPal obtained Class Members' consent to those disclosures;

E. Whether the data disclosed was identifiable to specific individuals;

F. Whether PayPal's representations regarding the privacy of Venmo transactions were false or misleading;

G. Whether PayPal's acts and practices violated the ECPA, 18 U.S.C. §§ 2510 *et seq.*;

H. Whether PayPal's acts and practices constituted an intrusion upon seclusion under the common law;

I. Whether PayPal's acts and practices violated Article I, Section 1 of the California Constitution;

J. Whether PayPal's acts and practices violated the CIPA, Cal. Penal Code §§ 630 *et seq.*;

K. Whether PayPal's acts and practices violated CDAFA, Cal. Penal Code § 502;

L. Whether PayPal's acts and practices violated the GLBA, 15 U.S.C. §§ 6801 *et seq.*;

M. Whether PayPal's acts and practices violated the CFIPA, Cal. Fin. Code §§ 4050 *et seq.*;

N. Whether PayPal's acts and practices violated the UCL, Cal. Bus. & Prof. Code §§ 17200 *et seq.*;

O. Whether PayPal was negligent;

P. Whether PayPal was unjustly enriched;

Q. Whether Plaintiffs and Class Members are entitled to equitable and injunctive relief, including restitution and disgorgement; and

R. Whether Plaintiffs and Class Members are entitled to actual, statutory, punitive, or other forms of damages.

149. ***Typicality.*** Plaintiffs' claims are typical of the claims of the other members of the Class and Subclass. Plaintiffs' claims and those of the Class and Subclass arise from the same conduct by PayPal and are based on the same legal theories.

150. ***Adequate Representation***. Plaintiffs will fairly and adequately represent and protect the interests of the Class and Subclass. Plaintiffs have retained counsel competent and experienced in complex litigation and class actions, including litigation to remedy privacy violations. Plaintiffs have no interest antagonistic to the interests of the Class and Subclass, and PayPal has no defenses unique to Plaintiffs. Plaintiffs and Plaintiffs' counsel are committed to vigorously prosecuting this action and have the resources to do so.

151. ***Superiority.*** A class action is superior to millions of individual cases filed by members of the Class and Subclass. The damages suffered by individual Class Members are small relative to the burden and expense of individual litigation, making it impracticable for Class Members to seek redress individually. This proposed class action presents fewer management difficulties than individual litigation and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

152. Rule 23(b)(2). PayPal has acted and refused to act on grounds generally applicable to the Class and Subclass, thereby making final injunctive relief and corresponding declaratory relief appropriate with respect to the Class and Subclass as a whole.

153. Plaintiffs reserve the right to revise the foregoing class allegations and definitions based on facts learned and legal developments following additional investigation, discovery, or otherwise.

CALIFORNIA LAW APPLIES TO THE CLASS AND SUBCLASS

154. California substantive law applies to every member of the Class and Subclass. California's substantive laws may be constitutionally applied to the claims of Plaintiffs and the Class under the Due Process Clause, U.S. Const. amend. XIV, § 1, and the Full Faith and Credit Clause, U.S. Const. art. IV, § 1. California has significant contacts, and a significant aggregation of contacts,

with the claims asserted by Plaintiffs and Class Members, thereby creating state interests that ensure the choice of California law is neither arbitrary nor unfair.

155. PayPal maintains its principal place of business in California and conducts substantial business in California. The decisions to incorporate the Tracking Technology into the Venmo Platform, to configure what data it transmitted, and to draft the representations alleged herein were made in California. California therefore has an interest in regulating PayPal's conduct under its laws.

156. The application of California law to the Nationwide Class and California Subclass is also appropriate under California's choice-of-law rules because California has significant contacts with the claims of Plaintiffs and the proposed Class and Subclass, and because California has a greater interest in applying its laws here—given PayPal's location and the location of the conduct at issue—than any other interested state.

CLAIMS FOR RELIEF

FIRST CLAIM FOR RELIEF
Violation of the Electronic Communications Privacy Act
18 U.S.C. §§ 2510 *et seq.*
(On Behalf of Plaintiffs and the Nationwide Class)

157. Plaintiffs re-allege and incorporate the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

158. The ECPA prohibits the intentional interception of, and the procuring of another person to intercept, the contents of any electronic communication, and the use of information obtained through such interception. 18 U.S.C. § 2511.

159. The ECPA protects both the sending and the receipt of communications and provides a private right of action to any person whose electronic communications are intercepted. 18 U.S.C. § 2520.

160. The transmissions between Plaintiffs and Class Members and PayPal—including the identity of the counterparty, the amount of the payment, and the note describing the purpose of the transaction—qualify as electronic communications under the ECPA. 18 U.S.C. § 2510(12).

161. These communications include "contents" within the meaning of 18 U.S.C. § 2510(8), because they concern the substance, purport, and meaning of the communication. The note field in particular is a free-text message authored by the user describing the purpose of the payment.

162. The Tracking Technology constitutes a "device" within the meaning of 18 U.S.C. § 2510(5).

163. At all relevant times, PayPal aided, employed, agreed with, and procured third parties, including at least mParticle and Kochava, to intercept Plaintiffs' and Class Members' communications on the Venmo Platform, and to use those intercepted communications. These communications were transmitted to and intercepted by third parties during the communication and without the knowledge, authorization, or consent of Plaintiffs and Class Members.

164. PayPal intentionally incorporated into the Venmo Platform code that, without Plaintiffs' and Class Members' knowledge or consent, captured and transmitted the substance of their confidential communications with PayPal to the Third-Party Recipients.

165. PayPal played an active role in this conduct. PayPal customized and deployed the Tracking Technology, and had full control over which screens contained it, what information was tracked and transmitted, and how events were configured and named prior to transmission.

166. The Tracking Technology is designed such that it transmits a user's actions and communications contemporaneously with the user's initiation of each communication. As a result, the communications were intercepted in transit to the intended recipient—PayPal—before reaching PayPal's servers.

167. The Third-Party Recipients are not parties to Plaintiffs' and Class Members' communications with PayPal. mParticle and Kochava would not have intercepted or received the

contents of these communications, or had access to them, but for PayPal's incorporation of the Tracking Technology into the Venmo Platform.

168. In aiding and permitting third parties to intercept its users' communications, PayPal acted for a purpose that was tortious. The unauthorized disclosure of private communications in order to profit from that information is tortious in and of itself. PayPal intentionally committed a tortious act by disclosing Plaintiffs' and Class Members' private financial communications to third parties without authorization, and by permitting those third parties to record and use that information in a manner that exceeds what PayPal represented to its users.

169. In aiding and permitting third parties to intercept its users' communications, PayPal further acted for a purpose designed to violate state and federal constitutional and statutory provisions, including:

A. a knowing intrusion upon Plaintiffs' and Class Members' seclusion;

B. Article I, Section 1 of the California Constitution;

C. CIPA, Cal. Penal Code §§ 630 *et seq.*;

D. CDAFA, Cal. Penal Code § 502;

E. GLBA, 15 U.S.C. §§ 6801 *et seq.*;

F. the CFIPA, Cal. Fin. Code §§ 4050 *et seq.*; and

G. the California Unfair Competition Law.

170. Plaintiffs and Class Members seek appropriate equitable and declaratory relief, including injunctive relief; actual damages and any profits made by PayPal as a result of its violations, or the appropriate statutory measure of damages; punitive damages in an amount to be determined by a jury; and reasonable attorneys' fees and other litigation costs reasonably incurred pursuant to 18 U.S.C. § 2520.

171. This includes monetary damages for the greater of (i) the sum of the actual damages suffered by Plaintiffs and Class Members and any profits made by PayPal as a result of the violation, or (ii) statutory damages of the greater of $100 a day for each day of violation or $10,000.

SECOND CLAIM FOR RELIEF
Invasion of Privacy — Intrusion Upon Seclusion
(On Behalf of Plaintiffs and the Nationwide Class)

172. Plaintiffs re-allege and incorporate the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

173. A plaintiff asserting a claim for intrusion upon seclusion must plead (1) that the defendant intentionally intruded into a place, conversation, or matter as to which the plaintiff had a reasonable expectation of privacy; and (2) that the intrusion was highly offensive to a reasonable person.

174. PayPal's disclosure of Plaintiffs' and Class Members' PII to the Third-Party Recipients constitutes an intentional intrusion upon Plaintiffs' and Class Members' solitude and seclusion.

175. Plaintiffs and Class Members had a reasonable expectation of privacy in their financial transaction data—including the identity of their counterparties, the amounts they paid, and the notes describing the purposes of their payments—and in the PII associated with their Venmo accounts. This information is inherently sensitive.

176. That expectation was heightened by PayPal's consistent representations that this information would be safeguarded and would not be disclosed to third parties, and by PayPal's provision of a per-transaction "Private" setting that PayPal represented would prevent any sharing beyond the counterparty.

177. Plaintiffs and Class Members did not consent to, authorize, or know about PayPal's intrusion at the time it occurred.

178. The surreptitious disclosure of private financial transaction data belonging to millions of individuals was highly offensive because it violated expectations of privacy established by social norms, by federal and state financial privacy law, and by PayPal's own express promises.

179. The offensiveness of PayPal's conduct is compounded by the fact that it was carried out in secret, through highly technical means that Plaintiffs and Class Members could not detect, and in direct contradiction of PayPal's representations.

180. As a direct and proximate result of PayPal's conduct, Plaintiffs and Class Members have suffered harm and injury, including but not limited to the invasion of their privacy rights and the loss of control over and value of their personal data.

181. Plaintiffs and Class Members seek appropriate relief for that injury, including damages that will reasonably compensate them for the harm to their privacy interests, as well as disgorgement of the profits PayPal made as a result of its intrusion.

182. Plaintiffs and Class Members are also entitled to punitive damages resulting from the malicious, willful, and intentional nature of PayPal's conduct, which was directed at injuring Plaintiffs and Class Members in conscious disregard of their rights. Such damages are needed to deter PayPal from engaging in such conduct in the future.

THIRD CLAIM FOR RELIEF
Invasion of Privacy — Article I, Section 1 of the California Constitution
(On Behalf of Plaintiffs and the California Subclass)

183. Plaintiffs re-allege and incorporate the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

184. Article I, Section 1 of the California Constitution provides: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy."

185. To state a claim for invasion of privacy under the California Constitution, a plaintiff must establish (1) a legally protected privacy interest; (2) a reasonable expectation of privacy under the circumstances; and (3) an intrusion so serious in nature, scope, and actual or potential impact as to constitute an egregious breach of social norms.

186. The right to privacy under the California Constitution creates a right of action against private as well as governmental entities.

187. Plaintiffs and California Subclass Members have, and continue to have, a legally protected privacy interest in their financial transaction data and PII, and a reasonable expectation of privacy in that information.

188. PayPal disclosed that information to third parties without Plaintiffs' and California Subclass Members' consent, for commercial purposes including analytics, attribution, and marketing. The manner in which PayPal disclosed this information defeated established privacy mechanisms—including the ECPA, CIPA, CFIPA, GLBA, and PayPal's own privacy settings—and social norms.

189. This conduct constitutes an extremely serious invasion of privacy that would be highly offensive to a reasonable person. Reasonable individuals do not expect that third-party data companies are intercepting the amounts they pay, the persons they pay, and their descriptions of why they are paying, let alone using that information for profit.

190. PayPal's conduct violated the privacy of Plaintiffs and California Subclass Members without their consent.

191. Plaintiffs and California Subclass Members seek damages to compensate the harm to their privacy interests, as well as disgorgement of the profits PayPal made as a result of its invasion of their privacy.

192. PayPal's conduct was willful, knowing, and carried out in conscious disregard of Plaintiffs' and California Subclass Members' rights. Plaintiffs and California Subclass Members are entitled to punitive and exemplary damages.

FOURTH CLAIM FOR RELIEF

Violation of the California Invasion of Privacy Act
Cal. Penal Code § 631
(On Behalf of Plaintiffs and the California Subclass)

193. Plaintiffs re-allege and incorporate the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

194. The California Legislature enacted CIPA, Cal. Penal Code §§ 630 *et seq.*, finding that "advances in science and technology have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications and that the invasion of privacy resulting from the continual and increasing use of such devices and techniques has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society." *Id*. § 630. The intent behind CIPA is "to protect the right of privacy of the people of this state." *Id.*

195. Cal. Penal Code § 631(a) imposes liability on any person who, "by means of any machine, instrument, or contrivance, or in any other manner" (1) "intentionally taps, or makes any unauthorized connection . . . with any telegraph or telephone wire, line, cable, or instrument"; (2) "willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state"; (3) "uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained"; or (4) "aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section."

196. PayPal is a "person" for purposes of Section 631.

197. The Tracking Technology, together with Plaintiffs' and California Subclass Members' computers and mobile devices, constitutes a "machine, instrument, or contrivance, or . . . other manner" under Section 631.

198. PayPal, by embedding, configuring, and enabling the Tracking Technology that captured the substance of Plaintiffs' and California Subclass Members' communications to the

Third-Party Recipients contemporaneously with transmission, aided, agreed with, employed, and conspired with the Third-Party Recipients to accomplish the unauthorized interception described herein, in violation of Section 631(a).

199. The code PayPal incorporated onto Plaintiffs' and California Subclass Members' devices and browsers tracked and transmitted the substance of their confidential communications with PayPal to the Third-Party Recipients, without Plaintiffs' or California Subclass Members' knowledge or consent. The Third-Party Recipients constitute "persons" within the meaning of the statute.

200. PayPal had full control over the Tracking Technology, including which screens contained it, what information was tracked and transmitted, and how events were configured prior to transmission, and used that control to facilitate the Third-Party Recipients' interception and collection of Plaintiffs' and California Subclass Members' PII, including transaction information such as recipient details and notes associated with each transaction. PayPal acted intentionally as only PayPal could modify its code to incorporate the Tracking Technology. mParticle, Kochava, and other Third-Party Recipients would not have been able to intercept or receive the contents of these communications but for PayPal's incorporation of the Tracking Technology into the Venmo Platform.

201. Separately, PayPal is liable under Section 631(a) also because it authorized and facilitated an interception of communications by parties—the Third-Party Recipients—whose receipt of those communications exceeded the scope of consent given by Plaintiffs and California Subclass Members. Plaintiffs and California Subclass Members did not consent and could not have consented to having their communications with PayPal simultaneously and secretly captured and provided to undisclosed third parties for those parties' own commercial purposes because PayPal policies specifically provided that those communications would not be disclosed.

202. PayPal failed to disclose its use of the Tracking Technology to track and automatically and simultaneously transmit Plaintiffs' and California Subclass Members' communications with PayPal to undisclosed third parties.

203. As a result of these violations, and pursuant to Cal. Penal Code § 637.2, PayPal is liable to Plaintiffs and California Subclass Members for three times their actual damages related to their loss of privacy in an amount to be determined at trial, or for statutory damages in the amount of $5,000 per violation, whichever is greater.

<u>FIFTH CLAIM FOR RELIEF</u>
Violation of the California Invasion of Privacy Act
Cal. Penal Code § 632
(On Behalf of Plaintiffs and the California Subclass)

204. Plaintiffs re-allege and incorporate the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

205. Cal. Penal Code § 632(a) imposes liability on any person who "intentionally and without the consent of all parties to a confidential communication, uses an electronic amplifying or recording device to eavesdrop upon or record the confidential communication."

206. Section 632(c) defines "confidential communication" to include "any communication carried on in circumstances as may reasonably indicate that any party to the communication desires it to be confined to the parties thereto."

207. Plaintiffs' and California Subclass Members' communications with PayPal—including the identity of their counterparties, the amounts of their payments, the notes describing the purposes of those payments, and their PII—were confidential communications for purposes of Section 632, because Plaintiffs and California Subclass Members had an objectively reasonable expectation that those communications would be confined to themselves, PayPal, and the counterparty.

208. That expectation is confirmed by PayPal's own representations, including its representation that a transaction marked "Private" would not be shared "anywhere other than in your personal transactions feed under the Me tab and with the other participant."[51]

209. PayPal, by embedding the Tracking Technology on the Venmo Platform, enabled the recording of Plaintiffs' private communications by unauthorized Third-Party Recipients in violation of Section 632.

210. Plaintiffs and California Subclass Members did not consent and could not have consented to having their communications with PayPal simultaneously and secretly captured and provided to undisclosed third parties for those parties' own commercial purposes because PayPal policies specifically provided that those communications would not be disclosed.

211. PayPal aided, abetted, agreed with, employed, and conspired with the Third-Party Recipients to accomplish this eavesdropping and recording by intentionally configuring the Venmo Platform to grant the Third-Party Recipients contemporaneous access to Plaintiffs' and California Subclass Members' confidential communications, in violation of Section 632.

212. Plaintiffs and California Subclass Members seek statutory damages in accordance with Cal. Penal Code § 637.2(a), which provides for the greater of (1) $5,000 per violation, or (2) three times the amount of actual damages sustained, in an amount to be proven at trial, as well as injunctive and other equitable relief.

SIXTH CLAIM FOR RELIEF
Violation of the California Comprehensive Computer Data Access and Fraud Act
Cal. Penal Code § 502
(On Behalf of Plaintiffs and the California Subclass)

213. Plaintiffs re-allege and incorporate the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

---

[51] Help Center, Manage your Venmo privacy settings, Venmo, https://help.venmo.com/cs/articles/manage-your-venmo-privacy-settings-vhel351 (last visited August 26, 2026).

214. The California Legislature enacted CDAFA to "expand the degree of protection afforded . . . from tampering, interference, damage, and unauthorized access to lawfully created computer data and computer systems," finding that "the proliferation of computer technology has resulted in a concomitant proliferation of . . . forms of unauthorized access to computers, computer systems, and computer data," and that "protection of the integrity of all types and forms of lawfully created computers, computer systems, and computer data is vital to the protection of the privacy of individuals." Cal. Penal Code § 502(a).

215. Plaintiffs' and California Subclass Members' devices—including their smartphones, tablets, and computers—on which PayPal installed the Third-Party Recipients' Tracking Technology constitute "computers," "computer systems," and "computer networks" within the meaning of CDAFA. *Id.* § 502(b).

216. The data PayPal accessed and disclosed from those devices constitutes "data" within the meaning of CDAFA. *Id.* § 502(b)(8).

217. PayPal violated Section 502(c)(1) by knowingly accessing and without permission using Plaintiffs' and California Subclass Members' devices, and placing cookies, identifiers, and other Tracking Technology on their devices and in local storage, in order to wrongfully obtain, disclose, and use their personal data in violation of their reasonable expectations of privacy in their devices and data.

218. PayPal violated Section 502(c)(2) by knowingly and without permission taking, copying, and making use of Plaintiffs' and California Subclass Members' unique identifiers, private transaction data, and other personal data from their devices.

219. Plaintiffs' and California Subclass Members' device functionalities, device systems, device networks, and browsers constitute "computer services" within the meaning of CDAFA. PayPal violated Section 502(c)(3) by knowingly and without permission causing those services to be used and accessed by third parties through the Tracking Technology and identifying mechanisms it incorporated into the Venmo Platform.

220. PayPal violated Section 502(c)(7) by knowingly and without permission causing Plaintiffs' and California Subclass Members' computers, computer systems, and computer networks to be accessed through the Tracking Technology and identifying mechanisms incorporated into the Venmo Platform.

221. PayPal violated Sections 502(c)(6) and (c)(13) by knowingly, and without permission from Plaintiffs and California Subclass Members, providing and/or assisting in providing the Third-Party Recipients with the means of accessing Plaintiffs' and California Subclass Members' devices, device systems, device networks, and browsers via the Tracking Technology and identifying mechanisms incorporated into the Venmo Platform.

222. Section 502(b)(12) defines a "computer contaminant" as "any set of computer instructions that are designed to . . . record, or transmit information within a computer, computer system, or computer network without the intent or permission of the owner of the information." The Tracking Technology PayPal incorporated into the Venmo Platform constitutes a computer contaminant as so defined. PayPal violated Section 502(c)(8) by knowingly and without permission introducing computer contaminants into Plaintiffs' and California Subclass Members' devices, device systems, device networks, and browsers, which intercepted and disclosed their PII, which includes transaction information such as recipient details and notes associated with each transaction, to third parties.

223. The Tracking Technology was deeply embedded in the Venmo Platform. Plaintiffs and California Subclass Members had no way to detect it, remove it, or opt out of its functionality.

224. Plaintiffs and California Subclass Members suffered damage and loss as a result of PayPal's conduct. PayPal's practices deprived them of control over their valuable property—namely, their PII, which includes transaction information such as recipient details and notes associated with each transaction—of the ability to receive compensation for that data, and of the ability to withhold that data from sale or disclosure.

225. PayPal's use of the Tracking Technology further harmed Plaintiffs and California Subclass Members by consuming additional bandwidth, processor time, data usage, storage, and battery power on their devices.

226. Plaintiffs and California Subclass Members seek compensatory damages in accordance with Cal. Penal Code § 502(e)(1), in an amount to be proven at trial, and injunctive and other equitable relief. Plaintiffs and California Subclass Members have suffered irreparable harm that will continue unless PayPal is enjoined from further violations, and have no adequate remedy at law.

227. Plaintiffs and California Subclass Members are entitled to punitive or exemplary damages pursuant to Cal. Penal Code § 502(e)(4) because PayPal's violations were willful and, upon information and belief, PayPal is guilty of oppression, fraud, or malice as defined in Cal. Civ. Code § 3294(c). Plaintiffs and California Subclass Members are also entitled to recover their reasonable attorneys' fees under Section 502(e)(2).

SEVENTH CLAIM FOR RELIEF
Violation of the California Unfair Competition Law
Cal. Bus. & Prof. Code §§ 17200 *et seq.*
(On Behalf of Plaintiffs and the California Subclass)

228. Plaintiffs re-allege and incorporate the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

229. PayPal's business acts and practices are "unlawful" under the UCL because, as alleged above, PayPal violated California common law and the federal and California statutes described herein, including the ECPA; CIPA; CDAFA; CFIPA; GLBA; and Article I, Section 1 of the California Constitution.

230. PayPal's business acts and practices are also "unfair" under the UCL. California has a strong public policy of protecting consumers' privacy interests, including their financial privacy, as reflected in Article I, Section 1 of the California Constitution, CIPA, CFIPA, and GLBA. PayPal violated that public policy by disclosing Plaintiffs' and California Subclass Members' PII, which

includes transaction information such as recipient details and notes associated with each transaction, without their consent.

231. PayPal's acts and practices are also "unfair" in that they are immoral, unethical, oppressive, unscrupulous, and substantially injurious to consumers. The gravity of the harm from PayPal's secret disclosure and misuse of Plaintiffs' and California Subclass Members' private financial data is significant, and there is no corresponding benefit to consumers. Because Plaintiffs and California Subclass Members were entirely unaware of PayPal's conduct, they could not possibly have avoided the harm.

232. PayPal's business acts and practices are also "fraudulent" within the meaning of the UCL. PayPal represented that it did not disclose users' personal information to third parties for promotional or marketing purposes; that only "public information" could be accessed through third-party services integrated with its products; that transactions marked "Private" would not be shared anywhere other than the user's personal transactions feed and with the counterparty; that users' financial information "stays secure";[52] and that, for accounts with California mailing addresses, PayPal would not share personal information except as permitted under California law.

233. These representations were false and were likely to deceive, and did deceive, members of the public, including Plaintiffs and California Subclass Members, into believing that their PII would not be disclosed to third parties.

234. PayPal omitted and concealed material facts it had a duty to disclose, given its exclusive knowledge of the Tracking Technology incorporated into the Venmo Platform, the data transmitted through that technology, and the uses to which that data was put.

235. Had Plaintiffs and California Subclass Members known that their PII, which includes transaction information such as recipient details and notes associated with each transaction, would be disclosed to and intercepted by third parties, they would not have used the Venmo Platform,

---

[52] Trust & Safety, A safe way to pay and get paid, Venmo, https://venmo.com/about/us/trust-and-safety (last visited August 26, 2026).

would not have provided their information to PayPal, or would have used the Venmo Platform differently and less frequently.

236. Plaintiffs and California Subclass Members have a property interest in their personal data, which has objective and ascertainable economic value. By surreptitiously disclosing that data, PayPal took property from Plaintiffs and California Subclass Members without providing just or any compensation, and PayPal derived revenue and other economic benefits as a result.

237. Plaintiffs and California Subclass Members have therefore suffered injury in fact and lost money or property as a result of PayPal's unfair competition.

238. To the extent this Court finds that Plaintiffs and the California Subclass have an adequate remedy at law for any of the conduct alleged in this Claim, Plaintiffs plead this Claim for equitable relief in the alternative and allege that legal remedies are inadequate to redress the full scope of PayPal's unlawful, unfair, and fraudulent conduct, including its ongoing and uncorrected data-sharing practices, for which injunctive relief is necessary and for which no adequate remedy at law exists.

239. Plaintiffs and California Subclass Members seek restitution, disgorgement, injunctive relief, and other equitable relief as a result of PayPal's violations of the UCL.

EIGHTH CLAIM FOR RELIEF
Unjust Enrichment / Quasi-Contract (Restitution)
(On Behalf of Plaintiffs and the Nationwide Class)

240. Plaintiffs re-allege and incorporate the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

241. PayPal received benefits from Plaintiffs and Class Members and unjustly retained those benefits at their expense.

242. PayPal received Plaintiffs' and Class Members' highly valuable PII, which includes transaction information such as recipient details and notes associated with each transaction, which

PayPal disclosed to, and permitted to be intercepted and recorded by, third parties, including the Third-Party Recipients, without authorization and without proper compensation.

243. PayPal used that data for its own gain, obtaining economic, intangible, and other benefits, including analytics regarding user behavior, attribution reporting measuring the effectiveness of its advertising expenditures, the ability to construct and target custom audiences, and improvement of its platform and marketing operations.

244. Had Plaintiffs and Class Members known of PayPal's conduct, they would not have provided their data to PayPal and would not have used the Venmo Platform.

245. PayPal unjustly retained these benefits at the expense of Plaintiffs and Class Members, whom PayPal's conduct damaged, without providing any commensurate compensation.

246. The benefits PayPal derived from Plaintiffs and Class Members rightly belong to Plaintiffs and Class Members. It would be inequitable under the unjust enrichment principles of California and every other state for PayPal to retain any of the profits or other benefits it derived from the unfair and unconscionable methods, acts, and practices alleged in this Complaint.

247. PayPal should be compelled to disgorge, into a common fund for the benefit of Plaintiffs and Class Members, all unlawful and inequitable proceeds it received, and to provide such other relief as the Court may deem just and proper.

NINTH CLAIM FOR RELIEF
Negligence
(On Behalf of Plaintiffs and the Nationwide Class)

248. Plaintiffs re-allege and incorporate the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

249. PayPal owed Plaintiffs and Class Members a common-law duty to exercise reasonable care in safeguarding their PII and in accurately describing its Privacy Statement. PayPal's standard of conduct is also set forth in the GLBA.

250. The GLBA 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." 15 U.S.C. § 6809(3)(A).

251. PayPal is a financial institution, as that term is defined by Section 509(3)(A) of the GLBA, 15 U.S.C. § 6809(3)(A), and is subject to the GLBA.

252. Among other things, PayPal 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)(5)(B)(ii).

253. PayPal is also significantly engaged in data processing and transmission, financial activities as described in 12 C.F.R. § 225.28(b)(14), as covered by the GLBA. PayPal collects nonpublic personal information, as defined by 16 C.F.R. § 313.3(n). Because PayPal is a financial institution that collects nonpublic personal information, 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 GLBA Safeguards Rule, 16 C.F.R. § 314.1 *et seq.*

254. Section 501 of the GLBA imposes on every covered financial institution, including PayPal, "an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information," and requires that various federal agencies and authorities establish appropriate standards that covered financial institutions must follow to fulfill their statutory obligation. 15 U.S.C. § 6801(a).

255. The Privacy Rule implements Sections 503-505 of the GLBA, 15 U.S.C. §§ 6803-6805, and was promulgated by the FTC on May 24, 2000. *See* 16 C.F.R. Part 313. The CFPB has promulgated the Privacy of Consumer Financial Information, Regulation P, 12 C.F.R. Part 1016 ("Reg. P").

256. 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(a) and 313.5(a)(1); 12 C.F.R. §§ 1016.4(a) and 1016.5(a)(1). "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(a) and 313.5(a)(1); 12 C.F.R. §§ 1016.4(a) and 1016.5(a)(1). 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(a); 12 C.F.R. § 1016.6(a);

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(a); 12 C.F.R. § 1016.9(a). 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).

257. PayPal violated both Reg. P and the Privacy Rule. PayPal's Venmo Privacy Statement was not accurate. Furthermore, as described above, PayPal failed to comply with these requirements through its sharing of Plaintiffs' and Class Members' PII with the Third-Party Recipients and the failure to disclose that sharing in its Privacy Statement.

258. PayPal's conduct violated the GLBA.

259. Plaintiffs and Class Members are consumers within the class of persons the GLBA was intended to protect.

260. Pursuant to Cal. Evid. Code § 669, a rebuttable presumption of negligence arises where a person violates a statute, the violation proximately causes injury of a kind the statute was designed to prevent, and the injured person was one of the class of persons the statute was designed to protect. Each of these elements is satisfied here: PayPal violated the GLBA, as alleged above; that violation proximately caused Plaintiffs and Class Members to have their sensitive information disclosed without consent; the harm suffered is precisely the type of harm the GLBA was designed to prevent; and Plaintiffs and Class Members, as consumers, are within the class of persons the GLBA was intended to protect.

261. The harm that has occurred as a result of PayPal's conduct is the type of harm that the GLBA was intended to guard against.

262. Plaintiffs' and Class Members' PII constitutes personal property that was taken and misused as a proximate result of PayPal's negligence, resulting in harm, injury, and damages to Plaintiffs and Class Members.

263. PayPal breached its duties to Plaintiffs and the Class under GLBA by failing to disclose that Plaintiffs' PII would be shared with the Third-Party Recipients.

264. As a proximate result of PayPal's negligence and breach of duties as set forth above, Plaintiffs and Class Members have suffered damages, *inter alia*, the sharing of their PII with Third-Party Recipients without their authorization or consent, fear, anxiety, and worry about the status of their PII, diminution in the value of their personal data for which there is a tangible value, and/or a loss of control over their PII, all of which can constitute actionable actual damages.

265. PayPal's conduct in violation of applicable laws directly and proximately caused the unauthorized access and disclosure of Plaintiffs' and Class Members' PII, and as a result, Plaintiffs and Class Members have suffered and will continue to suffer damages as a result of PayPal's conduct.

266. Plaintiffs and Class Members seek actual and compensatory damages, and all other relief they may be entitled to as a proximate result of PayPal's negligence. Plaintiffs and Class

Members are also entitled to punitive damages resulting from the malicious, willful, and intentional nature of PayPal's actions, directed at injuring Plaintiffs and Class Members in conscious disregard of their rights. Such damages are needed to deter PayPal from engaging in such conduct in the future.

TENTH CLAIM FOR RELIEF
Negligence
(On Behalf of Plaintiffs and the California Subclass)

267. Plaintiffs re-allege and incorporate the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

268. PayPal owed Plaintiffs and California Subclass Members a common-law duty to exercise reasonable care in safeguarding their PII and in accurately describing its Privacy Statement. PayPal's standard of conduct is also set forth in CFIPA.

269. The California Legislature enacted CFIPA, Cal. Fin. Code §§ 4050 *et seq.*, finding that "[t]he policies intended to protect financial privacy imposed by [the GLBA] are inadequate to meet the privacy concerns of California residents," Cal. Fin. Code § 4051.5(a)(3), and that California residents are entitled to "privacy protections that are stronger than those provided in federal law." Cal. Fin. Code § 4051.5(a)(4).

270. PayPal is a "financial institution" within the meaning of Cal. Fin. Code § 4052(c) and does business in California. PayPal holds itself out as such, including by delivering the Venmo Privacy Statement in the format prescribed for financial institutions' privacy notices.

271. Plaintiffs and California Subclass Members are "consumers" within the meaning of Cal. Fin. Code § 4052(f).

272. Plaintiffs' and California Subclass Members' PII, which includes transaction information such as recipient details and notes associated with each transaction—constitutes "nonpublic personal information" within the meaning of Cal. Fin. Code § 4052(a).

273. Plaintiffs' and California Subclass Members' PII meets the definition of "Personally identifiable financial information," under Cal. Fin. Code § 4052(b).

274. Cal. Fin. Code § 4052.5 prohibits a financial institution from disclosing nonpublic personal information to a nonaffiliated third party unless the consumer has consented in the manner prescribed by the statute.

275. PayPal disclosed Plaintiffs' and California Subclass Members' nonpublic personal information to nonaffiliated third parties, including mParticle and Kochava, without obtaining the consent required by CFIPA. PayPal never presented Plaintiffs or California Subclass Members with a disclosure form permitting them to consent to, or decline, the disclosures at issue. To the contrary, PayPal represented in its Privacy Statement that it did not share personal information with nonaffiliates.

276. PayPal designed and configured the transmissions at issue, controlled which data fields were included, and simultaneously represented to consumers that it did not engage in such sharing.

277. PayPal's conduct violated CFIPA.

278. Plaintiffs and California Subclass Members are consumers within the class of persons CFIPA was intended to protect.

279. Pursuant to Cal. Evid. Code § 669, a rebuttable presumption of negligence arises where a person violates a statute, the violation proximately causes injury of a kind the statute was designed to prevent, and the injured person was one of the class of persons the statute was designed to protect. Each of these elements is satisfied here: PayPal violated CFIPA, as alleged above; that violation proximately caused Plaintiffs and California Subclass Members to have their sensitive information disclosed without consent; the harm suffered is precisely the type of harm CFIPA was designed to prevent; and Plaintiffs and California Subclass Members, as consumers, are within the class of persons CFIPA was intended to protect.

280. The harm that has occurred as a result of PayPal's conduct is the type of harm that CFIPA was intended to guard against.

281. Plaintiffs' and California Subclass Member's PII constitutes personal property that was taken and misused as a proximate result of PayPal's negligence, resulting in harm, injury and damages to Plaintiffs and California Subclass Members.

282. PayPal breached its duties to Plaintiffs and the California Subclass under CFIPA by failing to disclose that Plaintiffs' PII would be shared with the Third-Party Recipients.

283. As a proximate result of PayPal's negligence and breach of duties as set forth above, Plaintiffs and California Subclass Members have suffered damages, *inter alia*, the sharing of their PII with Third-Party Recipients without their authorization or consent, fear, anxiety, and worry about the status of their PII, diminution in the value of their personal data for which there is a tangible value, and/or a loss of control over their PII, all of which can constitute actionable actual damages.

284. PayPal's conduct in violation of applicable laws directly and proximately caused the unauthorized access and disclosure of Plaintiffs' and California Subclass Members' PII, and as a result, Plaintiffs and California Subclass Members have suffered and will continue to suffer damages as a result of PayPal's conduct.

285. Plaintiffs and California Subclass Members seek actual and compensatory damages, and all other relief they may be entitled to as a proximate result of PayPal's negligence. Plaintiffs and California Subclass Members are also entitled to punitive damages resulting from the malicious, willful, and intentional nature of PayPal's actions, directed at injuring Plaintiffs and California Subclass Members in conscious disregard of their rights. Such damages are needed to deter PayPal from engaging in such conduct in the future.

DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury on all issues so triable.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs on behalf of themselves and the proposed Classes, respectfully request that the Court enter an order:

A. Certifying the Classes and Subclasses, and appointing Plaintiffs as the Classes' representatives and their counsel as Class Counsel;

B. Finding that PayPal's conduct was unlawful, as alleged herein;

C. Awarding declaratory and injunctive relief against PayPal, including invalidating the arbitration provision in the New User Agreement;

D. Awarding such injunctive and other equitable relief as the Court deems just and proper, including enjoining Defendant from the sharing of Plaintiffs' and Class Members' PII;

E. Awarding Plaintiffs and the Class Members statutory, actual, compensatory, consequential, punitive, and nominal damages, as well as restitution and/or disgorgement of profits unlawfully obtained;

F. Awarding Plaintiffs and the Class Members pre-judgment and post-judgment interest;

G. Awarding Plaintiffs and the Class Members reasonable attorneys' fees, costs, and expenses; and

H. Granting such other relief as the Court deems just and proper.

Dated: September 1, 2026

<u>*/s/ Amber L. Schubert*</u>

Amber L. Schubert #278696
Sonum Dixit #353395
Of Counsel
AYLSTOCK WITKIN
KREIS & OVERHOLTZ PLC
17 E. Main Street, Suite 200
Pensacola, FL 32502
Tel: 850.202.1010
aschubert@awkolawllp.com
sdixit@awkolawllp.com

Christian Levis (*pro hac vice* forthcoming)
Patricia Zapata Latzer (*pro hac vice* forthcoming)
LOWEY DANNENBERG, P.C.

44 South Broadway, Suite 1100
White Plains, NY 10601
Tel: (914) 997-0500
Fax: (914) 997-0035
clevis@lowey.com
platzer@lowey.com

Anthony M. Christina (*pro hac vice* forthcoming)
LOWEY DANNENBERG, P.C.
One Tower Bridge
100 Front Street, Suite 520
West Conshohocken, PA 19428
Tel: (215) 399-4770
Fax: (914) 997-0035
achristina@lowey.com

Counsel for Plaintiffs and the Proposed Classes