

STATE OF HAWAI'I
Melina Sanchez 6613
Office of Consumer Protection
235 South Beretania Street, Room 801
Honolulu, Hawai'i 96813-2419
Telephone: (808) 586-2636

Electronically Filed
FIRST CIRCUIT
1CCV-22-0001610
20-DEC-2022
08:28 AM
Dkt. 1 CMPS

Of Counsel:
CRONIN, FRIED, SEKIYA,
KEKINA & FAIRBANKS
L. RICHARD FRIED, JR. 764-0
PATRICK F. McTERNAN 4269-0
600 Davies Pacific Center
841 Bishop Street
Honolulu, Hawai'i 96813
Telephone: (808) 524-1433

COHEN MILSTEIN SELLERS & TOLL PLLC
EMMY L. LEVENS (*Pro Hac Vice Motion Pending*)
PETER KETCHAM-COLWILL (*Pro Hac Vice Motion Pending*)
1100 New York Avenue, NW, Fifth Floor
Washington, DC 20005
Telephone: (202) 408-4600

Attorneys for Plaintiff State of Hawai'i
Office of Consumer Protection

THE CIRCUIT COURT OF THE FIRST CIRCUIT

STATE OF HAWAI'I

STATE OF HAWAI'I, by its Office of
Consumer Protection,

Plaintiff,

vs.

PAYPAL, INC., a Delaware corporation, and
PAYPAL HOLDINGS, INC., a Delaware
corporation,

Defendants.

Civil No. _____
(Other Civil Action)

COMPLAINT; SUMMONS TO ANSWER
CIVIL COMPLAINT

TABLE OF CONTENTS

COMPLAINT 1

INTRODUCTION 1

PARTIES 4

VENUE AND JURISDICTION 5

FACTS 6

 I. BACKGROUND 6

 II. DEFENDANT DECEPTIVELY AND UNFAIRLY FREEZES
 CONSUMERS’ ACCOUNTS AND SEIZES CONSUMERS’ FUNDS
 WITH NO NOTICE OR RECOURSE 7

 A. Defendant Deceptively and Unfairly Claims that Consumers Can
 Freely Access and Control Account Funds..... 8

 B. Defendant’s Unfair Freeze-and-Seize Practices Cause Substantial
 Injury to Hawai’i Consumers..... 15

 C. Defendant Fails to Adequately Disclose its Freeze-and-Seize
 Practices. 16

 III. DEFENDANT DECEPTIVELY FAILS TO PROTECT CONSUMERS
 FROM, OR RESPOND TO, FRAUD ON ITS PLATFORMS. 19

 IV. DEFENDANT’S PURCHASE PROTECTION PROGRAMS DECEIVE
 CONSUMERS AND UNFAIRLY ASSESS FEES WITHOUT NOTICE. 25

 A. Defendant Deceptively Promises Venmo Users Full Refunds When
 They “Turn On” Purchase Protection. 26

 B. Defendant Unfairly Charges Consumers a Purchase Protection Fee
 for Transactions that Do Not Qualify for Purchase Protection..... 32

 V. DEFENDANT DECEPTIVELY AND UNFAIRLY VIOLATES
 CONSUMER PRIVACY AND FACILITATES FRAUD BY MAKING
 VENMO ACCOUNT INFORMATION PUBLIC. 34

 A. Defendant Deceptively Promises Venmo Users Privacy While
 Making Their Financial Information Public by Default. 36

 B. Defendant Deceptively Claims That Venmo Users’ Account and
 Contacts Information Is Used for Limited Purposes..... 41

 C. Defendant Deceptively Failed to Disclose that It Broadcast Venmo
 Users’ Personally Identifiable Transaction Data via a Public API. 50

 D. Defendant Misrepresents Venmo Users’ Ability to Protect the
 Privacy of Past Transactions. 53

VIOLATIONS OF LAW	55
PRAYER FOR RELIEF	59

COMPLAINT

Plaintiff State of Hawai‘i, by its Office of Consumer Protection (“**State**” or “**Plaintiff**”), for a cause of action against the above-named Defendants, alleges and avers the following:

INTRODUCTION

1. The State brings this action against Defendants PayPal, Inc. and PayPal Holdings, Inc. (collectively, “**PayPal**” or “**Defendant**”) in order to protect Hawai‘i consumers from unfair and deceptive acts and practices in violation of Hawaii’s consumer protection laws.

2. Defendant owns and operates two electronic payments platforms: one which bears its own name, PayPal (the “PayPal Platform”), and another known as Venmo (the “Venmo Platform”) (collectively, the “Platforms”). Both platforms allow consumers to electronically transfer money to other consumers and businesses through mobile applications and websites.

3. With 397 million active consumer accounts, PayPal is a giant in the electronic payment industry. In 2021 alone, Defendant processed 19.3 billion transactions across its PayPal and Venmo Platforms, with a total payment volume of \$1.25 trillion—approximately 61 percent of which, or \$762.5 billion, occurred in the United States. Defendant’s active accounts include nearly 90 million Venmo accounts.

4. Defendant’s scale was further boosted by the COVID-19 pandemic, which drove a massive increase in electronic payments worldwide. The PayPal and Venmo Platforms, already giants in the online and mobile payments space, took advantage of the turbocharged need for socially distanced electronic financial technology. Defendant leaned heavily into consumers’ mass migration from brick-and-mortar financial services into e-payments, rolling out services like debit cards, credit products, and direct deposit.

5. As a result of these trends and Defendant’s own efforts, consumers increasingly rely on Defendant to manage their finances, safeguard their money, and protect their financial

information. Defendant has abused this position of trust by engaging in deceptive and unfair business practices that mislead and substantially injure Hawai‘i consumers, including: (1) freezing and seizing users’ funds without notice or effective recourse on the PayPal and Venmo Platforms; (2) misrepresenting the extent to which it protects users from fraud on the PayPal and Venmo Platforms; (3) deceptively offering “Purchase Protection” (on the Venmo Platform), and unfairly charging Purchase Protection fees for transactions where Purchase Protection is unavailable (on the PayPal and Venmo Platforms); and (4) deceptively and unfairly violating the privacy of consumers (on the Venmo Platform).

6. On both its Platforms, Defendant promises consumers that they will have instant access to their account funds. In reality, Defendant freezes consumer accounts and seizes user funds using automated processes, without notice, without explanation, and without providing any effective recourse. This practice deprives consumers of access to their funds—often needed to pay for rent and other critical necessities—for six months or more.

7. Defendants’ freeze-and-seize practices disproportionately affect some of Hawaii’s most vulnerable consumers: the unbanked and underbanked (collectively, “unbanked”). Unbanked households are those that lack consistent, affordable access to traditional banking services. A 2019 FDIC study reported that almost *20 percent* of Hawaii’s residents qualified as unbanked. Unbanked households are twice as likely to use services like PayPal and Venmo to conduct core financial transactions like paying bills as compared households with access to traditional banking options.

8. Defendant also deceives consumers regarding the extent to which it protects them from fraud. Defendant knows that fraud is rampant on the Venmo and PayPal Platforms—indeed, earlier this year, it acknowledged the existence of 4.5 million fake PayPal and Venmo accounts.

9. Defendant leads consumers to believe that it is broadly protecting them from fraudulent transactions on its Platforms and that it will provide assistance to consumers victimized by this fraud. In reality, Defendant’s so-called fraud protection only covers a narrow sliver of the extensive financial fraud occurring on its Platforms and leaves the countless consumers who are scammed into transferring money to fraudsters without recourse to recover their funds. According to a 2021 survey of scammed consumers by the Better Business Bureau, *only 14 percent* of scammed Venmo users were able to recover their funds. The other 86 percent were left without any recourse.

10. Adding insult to injury, one of the features Defendant offers to protect consumers from fraud—its so-called “Purchase Protection”—is unfair and deceptive. On the Venmo Platform, Defendant advertises that consumers can “turn on” Purchase Protection to receive a “full refund” if purchases of goods or services go awry. In fact, Defendant’s Purchase Protection is available only for a small subset of goods and services transactions, and “turning on” Purchase Protection only entitles consumers to apply for a refund—it does not guarantee one. Additionally, when a consumer selects the Purchase Protection option when sending money through either the PayPal or Venmo Platforms, the recipient is automatically charged a fee—whether or not the transaction was, in fact, a payment for goods and services “eligible” for Purchase Protection. Defendant provides no way for the recipient to recover incorrectly charged Purchase Protection fees—Defendant simply pockets this money, having charged for an illusory protection that is not available on most transactions.

11. Finally, Venmo’s very design deceptively and unfairly violates consumer privacy. The default settings on the Venmo Platform share consumers’ personally identifiable financial information publicly. This information—which includes consumers’ names, account user names,

profile pictures, contact lists, and transaction data—is published not just on Venmo, but is made available to anyone on the Internet. This practice is likely to mislead reasonable consumers, who expect financial institutions to maintain basic levels of privacy with respect to their personally identifiable financial information. It also contradicts Defendant’s own representations about how it uses consumers’ personal information, and unfairly leaves consumers vulnerable to the wide array of fraud on the Venmo Platform.

12. The cumulative effect of Defendant’s misconduct, which is directed at Hawai‘i consumers and occurs in Hawai‘i, has deprived Hawai‘i consumers of reliable access to their own money; rendered them vulnerable to, and in fact, the victims of, fraud; and undermined their ability to protect their own privacy and make informed decisions regarding the electronic payments services they wish to use. The State of Hawai‘i brings this action to permanently enjoin these unfair and deceptive practices and to secure all available civil penalties and equitable relief.

PARTIES

13. The State of Hawai‘i Office of Consumer Protection (“**OCP**”) is, in addition to the Office of the Attorney General, the civil law enforcement agency charged with the enforcement of Hawaii’s consumer protection laws, including but not limited to those statutes pertaining to the prevention of unfair or deceptive acts or practices in the conduct of any trade or commerce.

14. Defendant PayPal, Inc. is a Delaware corporation with its principal place of business at 2211 North First Street, San Jose, California 95131. PayPal, Inc. operates the Venmo Platform and the PayPal Platform, electronic payment services that allow consumers to make peer-to-peer payments and pay merchants. At all relevant times, PayPal, Inc. has been registered to do business in the State of Hawai‘i and has marketed and operated the Venmo Platform in the State of Hawai‘i. PayPal, Inc. holds a Hawai‘i Money Transmitter License and is a wholly-owned subsidiary of PayPal Holdings, Inc.

15. Defendant PayPal Holdings, Inc. is a Delaware corporation with its principal place of business at 2211 North First Street, San Jose, California 95131. PayPal Holdings, Inc. is the parent of PayPal, Inc. and holds all of assets and liabilities of PayPal, Inc. At all relevant times, PayPal Holdings, Inc. has been registered to do business in the State of Hawai‘i.

VENUE AND JURISDICTION

16. This action is brought by OCP pursuant to HRS Chapters 480, 481A, and 487, and seeks declaratory and injunctive relief, restitution, disgorgement, non-compensatory civil penalties, and any other additional relief against Defendant as the circumstances may warrant.

17. OCP is authorized to bring this action in the name of the State of Hawai‘i pursuant to HRS chapter 487 and § 480-15.

18. Subject matter jurisdiction for this case is conferred upon this Court pursuant to HRS § 603-21.5(3). Defendant is subject to personal jurisdiction in this Court pursuant to HRS § 634-35(a) because the causes of action asserted herein arose from Defendant’s transaction of business in Hawai‘i and from Defendant’s commission of unfair and deceptive trade practices in Hawai‘i, including the City and County of Honolulu, State of Hawai‘i.

19. The State brings this action exclusively under the laws of the State of Hawai‘i. No federal claims are being asserted, and to the extent that any claim or factual assertion set forth herein may be construed to have stated any claim for relief arising under federal law, such claim is expressly disavowed and disclaimed by the State.

20. Venue for this action is proper because Defendant is alleged to have committed violations of law within the City and County of Honolulu, State of Hawai‘i at all times relevant to this complaint.

FACTS

I. BACKGROUND

21. Electronic payments, or e-payments, allow consumers to convey money to another party—for personal or business transactions—electronically, as opposed to with cash or a paper check.

22. PayPal launched the PayPal Platform in 1998 as one of the first digital e-payment services. While the PayPal Platform began as a payments service, it has since attained “super-app” status,¹ expanding into a one-stop-shop for payments and financial services including credit and debit cards, a digital credit line, a high-yield savings account, a direct deposit feature that allows consumers to deposit paychecks and government payments, the ability to deposit paper checks, and a “bill pay” feature that allows consumers to manage bill payments, among others. When selected, these products and services are all linked to a consumer’s PayPal Platform account.

23. PayPal acquired its then-competitor, Braintree, which owned the Venmo Platform, in December 2013. After the acquisition, PayPal continued to operate the Venmo Platform as a separately branded platform.

24. The Venmo Platform, which started as a peer-to-peer payments platform, has similarly expanded the financial services it offers, which include credit and debit cards and a direct deposit feature. Defendant has announced plans to add many of the same financial services offered on the PayPal Platform to the Venmo Platform.

25. When a consumer uses the PayPal or Venmo Platforms to *receive* money, the funds are deposited into the consumer’s account balance. If a consumer takes no action, received funds

¹ A “super-app” refers to an application of platform that provides multiple different services and products in addition to just facilitating payments.

remain in the account balance. Consumers can transfer funds from their PayPal or Venmo account balance to a linked bank account, other PayPal or Venmo users, or merchants. When a consumer uses PayPal or Venmo to *send* money, the consumer can elect to use funds held in the consumer's PayPal or Venmo account balance or draw from a linked external bank account, debit card, or credit card.

26. The user interface experience on Defendant's respective Platforms is generally consistent across the United States—that is, the Venmo Platform generally looks and operates the same way in Hawai'i as it does in Maine or Montana, as does the PayPal Platform. This consistent user interface experience is a reflection of business imperatives including brand consistency, ease of operation across user channels, and streamlining Platform updates.²

II. DEFENDANT DECEPTIVELY AND UNFAIRLY FREEZES CONSUMERS' ACCOUNTS AND SEIZES CONSUMERS' FUNDS WITH NO NOTICE OR RECOURSE.

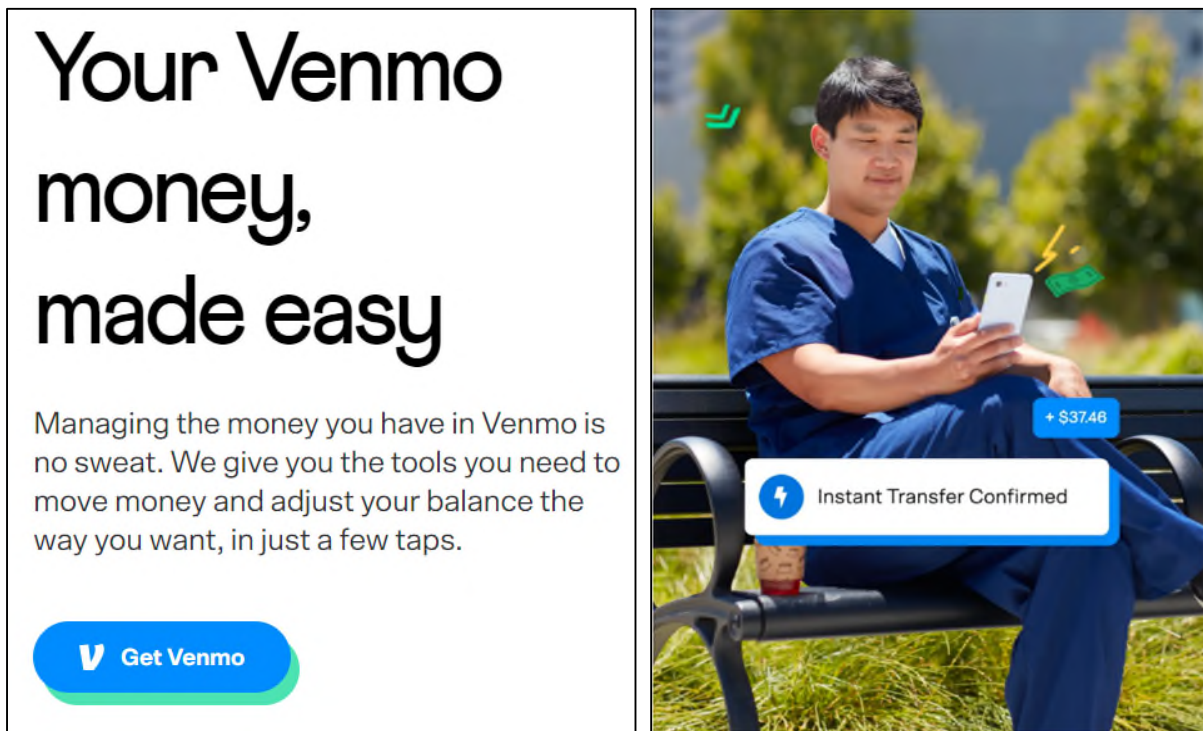
27. Defendant's expansion into many financial services traditionally offered by banks, along with the exigencies of the COVID-19 pandemic, have made the PayPal and Venmo Platforms increasingly central to how consumers manage their finances—including meeting critical obligations like paying rent and other bills.

28. Defendant has encouraged this transition by deceptively promising consumers the ability to access, on demand, account funds on the PayPal and Venmo Platforms. The truth is that Defendant deploys draconian freeze-and-seize practices that unfairly deprive consumers of access to their accounts and funds using an automated process and without notice or recourse.

² Across operating systems, the user experience may differ slightly to accommodate the familiarity of an iPhone user with iPhone user interface designs, and likewise with Android users.

A. Defendant Deceptively and Unfairly Claims that Consumers Can Freely Access and Control Account Funds.

29. On both its Platforms, Defendant deceptively tells users that they will have free and ready access to and control of their funds. For example, Defendant advertises that Venmo “give[s] you the tools you need to move money and adjust your balance the way you want,” “gives you the flexibility and control to help manage your money, your way,” and that users can “[m]ove money from Venmo to your bank account anytime.”



30. Other statements similarly represent that Venmo users are always able to access and control their Venmo account funds. For example, Defendant advertises on its website that users can “[s]end money in Venmo to a linked bank account anytime, at no charge.” On another page, Defendant says Venmo users can “[m]ove money between Venmo and your bank account, so your cash is exactly where you want it, when you want it.”

31. Defendant makes similar misrepresentations about PayPal accounts. The PayPal website advertises that “[y]our money goes right to your account. It can be ready when you need

it.” Under the heading “Flexible,” Defendant assures consumers that PayPal users can “[u]se your funds to shop online...or transfer it to your bank account.” On another webpage, it tells consumers they can “[t]ransfer your money your way,” with “Standard Transfer” service providing bank transfers in 1 to 3 business days “if your money can wait” and “Instant Transfer” service “[i]f you need your money now.”

32. Defendant’s representations deceptively convey that Venmo and PayPal users have control over, and access to, their account funds at all times. However, Defendant freezes Venmo and PayPal accounts unilaterally, without human review and without notice, depriving consumers of access to their own funds for *six months or more*. In some cases, Defendant then permanently deactivates the accounts, and rather than return the funds to the owner of the closed account, holds the account funds for six months. Additionally, Defendant will simply take possession of a Venmo or PayPal user’s account funds if, for example, Defendant believes the user owes Defendant money (*e.g.*, if a consumer stops payment on a transfer funded by a linked bank account), suspects the user has violated its Acceptable Use Policy, or if Defendant determines the user could subject Defendant to liability (*e.g.*, suspected fraud). Defendant provides consumers with no formal appeals process to recover their funds, leaving them struggling to reach customer service representatives that have no authority to reverse Defendant’s actions.

33. Defendant gives itself the right to freeze (and in fact does freeze) user accounts and seize account balances if it unilaterally determines that a consumer has violated its Platforms’ respective User Agreements. These bloated legal documents, which each contain more than 20,000 words, provide Defendant with an extensive list of possible justifications for depriving users of their funds that are so broad and subjective as to give Defendant almost total discretion in deciding when it can seize consumer funds. The “restricted activities” that Defendant deems to be violations

of its User Agreements include owing money to Defendant,³ violating a separate Acceptable Use Policy, and a broad, vague prohibition on using Defendant's services "in a manner that results in or may result in complaints, disputes, claims, reversals, chargebacks, or fees...or other liability or losses to [Defendant]...other customers, third parties, or you."⁴

34. Defendant also gives itself the right to freeze accounts if it, "in our sole discretion," "believe[s]" that a user, the user's account, or the user's transactions "may" present a "high level of risk," and if Defendant detects what it unilaterally judges to be "unusual or suspicious" activity.

35. Defendant freezes accounts without giving prior warning or notice to the affected consumer. These freezes can last 180 days, depriving consumers of the use of their funds for six months.

36. Defendant freezes user accounts using an automated process, without human review. Reports indicate that these automated freezes have been triggered by factors including transaction size and frequency, a consumer's description of the transaction, and whether the transaction causes the consumer to owe money to Defendant. These are just a handful of the reasons for which Defendant may freeze users' accounts.

37. Human "account specialists" or "limitation specialists" only review consumer account activity *after* the Defendant's automated system has frozen the account. These reviews have resulted in the permanent deactivation of consumer accounts, including in Hawai'i.

³ Consumers may end up owing money to Defendant because of the way Venmo and PayPal transactions work. When a consumer uses a linked bank account to send money using Venmo, for example, Defendant immediately transfers funds into the recipient account. Because it can take a day or more for the bank transfer to clear, if there are problems in the interim, such as a bank payment failure, the user may end up owing Defendant for the funds Defendant advanced on the user's behalf.

⁴ These statements do not appear until word 11,967 in the current Venmo User Agreement and at word 11,921 in the current PayPal User Agreement.

Following these deactivations, Defendant holds the funds for up to 180 days “to protect [PayPal] from potential financial losses,” though consumers have reported being unable to recover these funds even after 180 days.

38. In one example, a Hawai‘i consumer reported that their PayPal account was put on hold after using their PayPal “Cash Card” to make an in-store purchase. This account freeze deprived the consumer of access to \$17,000 of unemployment funds that had been deposited into the consumer’s PayPal account at the height of the covid-19 pandemic. In another, a consumer reported losing access to \$18,000 in their Venmo balance after Venmo froze and then permanently closed their account. At the time of the complaint, the consumer had been unable to access their funds for 5 months.

39. When a consumer requests additional information or clarification regarding the reason their accounts were frozen or deactivated, Defendant’s policy is to refuse to provide an explanation. According to Defendant, it cannot “divulge certain levels of decision-making criteria about account restrictions to protect the systems that monitor activity on its platform.” News reports and consumer complaints indicate that Defendant’s explanations for freezes and account deactivation are limited to vague language stating that the affected accounts were flagged for “potential risk” or that they violated Defendant’s User Agreements, without any explanation as to why or how.

40. One Hawai‘i consumer reported that PayPal terminated their account just three days after it was created, for activity that was allegedly inconsistent with its User Agreement—even though the only account activity during the three days was the receipt of a few payments from friends. PayPal refused to explain how the User Agreement was violated and provided no way to recover the money in the account.

41. Defendant's refusal to explain why it has frozen consumer funds violates public policy, which requires financial institutions such as PayPal to investigate a consumer's request for additional information or clarification concerning problems with an electronic fund transfer, and to communicate a full and clear explanation of its findings and determination.

42. One Hawai'i consumer reported that Defendant closed their PayPal account "for no reason," subjecting the account to a 180-day hold that ended up lasting even more than 180 days and "affected my ability to pay for basic expenses." Another Hawai'i consumer reported that Defendant terminated their PayPal account without warning based on unexplained "suspicious" activity, leaving the consumer unable to access the \$3,500 remaining in the account.

43. Hawai'i consumers have reported similar experiences with the Venmo Platform. In one case, the consumer's account was suspended "randomly and without reason," depriving them of access to over \$1,200. Venmo's customer support told the consumer that the only way to address the problem was by email.

44. Another Hawai'i consumer reported that their account was frozen, first temporarily and then permanently, after attempting to transfer money from their Venmo balance to their bank account. When the consumer asked for the reason the account was frozen, Venmo customer support refused to provide one, saying only that the action was taken at Venmo's discretion.

45. Even when Defendant freezes accounts and blocks user access to the funds, it still allows deposits into frozen accounts, exacerbating the harm to consumers. One Hawai'i consumer reported in September 2020 that Defendant froze her PayPal account without notice. While the account was frozen, Defendant allowed deposits to continue coming in, but prevented bills she had set to be paid automatically from her PayPal account from going out, causing her to incur late fees

on those bills. “They won’t let any transactions go through, [e]xcept deposits. How convenient for them. How horrible this is for the consumer.”

46. Defendant does not only freeze user accounts. If Defendant determines that a consumer owes it money for whatever reason, Defendant seizes the funds from the consumer’s account without warning. And, for consumers on the Venmo Platform, if a consumer’s account does not contain enough funds to cover the amount Defendant believes it is owed, Defendant reaches into the consumer’s PayPal account and takes the money from there. No reasonable consumer would expect their financial institution to seize their funds without notice—much less that it would seize the funds from an entirely separate account on a different platform.

47. In one example, Defendant seized \$440 from a Hawai‘i consumer’s Venmo account after the consumer was tricked into sending money to fraudsters via Venmo. After discovering they had been scammed, the consumer stopped payment on their linked bank account and attempted to notify Venmo of the fraud. Defendant transferred money to the scammer anyway—and because the consumer had stopped payment on the linked bank account, Defendant withdrew the \$440 from the consumer’s existing Venmo balance to fund the transfer. The consumer had intended to use the funds Defendant seized to pay the security deposit for their child’s college housing.

48. Until in or around October 29, 2022, Defendant also seized consumer funds in connection with a liquidated damages clause buried in its Acceptable Use Policy, which authorized Defendant unilaterally to collect \$2,500 per violation “directly from your PayPal account(s).” Numerous consumer complaints indicate Defendant used this clause to justify seizures of account funds bearing no relation to Defendant’s purported actual damages.

49. Defendant provides no clear or effective process for users to appeal or dispute its decisions to freeze, permanently deactivate, or seize funds from user accounts, leaving consumers to navigate a convoluted and ineffective customer support process. Media reports and consumer complaints—both in Hawai‘i and nationally—consistently report that customer support is difficult to reach, and if reached, is unwilling, unauthorized, or unable to provide an explanation or resolution of the issue. As reported by the *Wall Street Journal*, the Venmo Platform “deactivated general customer-service telephone lines during the pandemic.”

50. These reports further indicate that Defendant directs consumers who call customer support to use email instead, but does not timely respond to emailed support requests, leaving some consumers with “dayslong lags in email communication.” When Defendant permanently deactivates a consumer’s Venmo account, Defendant’s emails informing the consumer their account has been deactivated expressly state that “future contact or inquiries will not be answered.”

51. While Defendant claims that its freeze-and-seize practices are efforts to prevent fraud, the real goal of these deceptive and unfair practices appears to be protecting Defendant’s bottom line at the consumer’s expense. Only in its dense User Agreements does Defendant reveal the truth: that account freezes are “needed to protect against the risk of liability” and “monetary loss to [Defendant].”

52. Defendant’s freeze-and-seize practices, which deprive consumers of access to and control over their funds, are material to consumers. Consumer complaint databases are littered with reports about Defendant’s account-freezing practices. The Consumer Financial Protection Bureau’s Consumer Complaint Database contains over 2,500 complaints about frozen Venmo and PayPal accounts. Of the 100 most recent complaints to the Better Business Bureau about PayPal

and Venmo—of which over 35,000 have been filed in the past three years alone—more than half relate to Defendant’s freeze-and-seize practices.

B. Defendant’s Unfair Freeze-and-Seize Practices Cause Substantial Injury to Hawai‘i Consumers.

53. Defendant’s unfair practice of freezing and seizing user funds causes substantial injury to consumers, including by depriving consumers of the ability to access and use their own money. Many consumers have reported that their inability to access Venmo and PayPal account funds has caused them significant financial harm, including the inability to pay rent or other critical bills or receive child support payments.

54. This harm is compounded for those consumers who use the Venmo and PayPal Platforms’ direct deposit services, for whom account freezes and deactivations also means the loss of access to their paychecks or unemployment payments.

55. Defendant’s Platforms are widely used by lower-income adults. According to a PEW Research Study, 48 percent of lower-income adults use PayPal, and 26 percent of lower-income adults use Venmo. For these households, ready access to Platform funds can be critically important to meet daily needs. Unbanked households, many of which are also low-income households, are twice as likely as banked households to use services like PayPal and Venmo to conduct core financial transactions, like receiving income and paying bills.

56. Defendant is aware that its users depend on having access to their money stored on the Platforms for these sorts of core life expenses. Defendant’s President and CEO, Daniel Schulman, told investors in May of 2020,

We [added] things like direct deposit, so people can put their paycheck directly on to Venmo, because they’re using it now in all these different ways and so that they could receive their stimulus check right to their Venmo wallet as well. So it’s been really interesting to watch the evolution of Venmo become much more

central to people's management and movement of money, instead of just being a social payment.

57. Defendant actively encourages consumers to rely on its Platforms for critical payments through its advertising strategy, which highlights that consumers can use its services to pay for “utilities, rent, [and] groceries.”

58. Defendant has long known that its freeze-and-seize practices harm consumers by depriving them of access to their own money. Defendant has faced class action claims over these practices since 2010.

59. In its May 2018 administrative complaint against Defendant, the Federal Trade Commission (“FTC”) noted that “[m]any thousands of consumers” had complained about delays or loss of funds from their Venmo accounts, and that “many” consumers “reported suffering significant financial hardship.” Defendant’s internal emails going back to 2015 made clear that Defendant was aware of “user frustration” and confusion caused by freezing accounts.

60. Consumers cannot reasonably avoid the injuries caused by Defendant’s freeze-and-seize practices because Defendant does not adequately disclose this conduct, nor provide advance notice before freezing or seizing user funds. Consumers have no visibility into, or control over, Defendants’ opaque and unilaterally implemented internal policies, procedures, and systems.

C. Defendant Fails to Adequately Disclose its Freeze-and-Seize Practices.

61. At no point does Defendant adequately disclose to users that they can be deprived of access to, or possession of, their money without notice or a clear and effective method of appeal. Language disclosing Defendant’s freeze-and-seize practices does not appear on any of the sign-up screens consumers must navigate to create a Venmo or PayPal account. And the Platforms’ user transaction flows, in which a user sends or requests payment to or from another Venmo or PayPal user, contain no language disclosing this practice.

62. The only place on either Platform that Defendant provides information about its freeze-and-seize practices within the user flow is on the Venmo Platform, on a single screen allowing Venmo users to transfer their balances to a linked bank account. Venmo users who do not transfer their Venmo account balances to a linked bank account, and instead maintain Venmo account balances to conduct Venmo transactions, would not see this information at all.

63. For the subset of consumers who elect to transfer their Venmo balances to a linked bank account, the freeze-and-seize information appears in small font at the bottom of the screen, just above a “Transfer” button. In relevant part, it states: “Transfers are reviewed which may result in delays or funds being frozen or removed from your account. Learn more...” This language does not adequately disclose the material facts of Defendant’s freeze-and-seize practices, including that Defendant’s automated processes review all transactions, not just transfers; that such freezes can last six months or more; that Defendant freezes accounts based on alleged violations of its User Agreements, and not just to protect against fraud; and that Defendant offers no effective way to dispute such actions, among others.

64. The words “Learn more” link to a help page innocuously titled “Bank Transfer Timeline.” After information about the time required to complete a bank transfer, the same single-sentence disclaimer appears, followed by another “learn more” link at the end of the paragraph.

65. Only if a consumer clicked on this second “learn more” link would they be directed to a third screen: a Venmo Help Center page titled “Reviews of Transfers Into and Out of Venmo,” which states that Defendant reviews account and transaction activity for “suspicious or illegal activity” and non-compliance with the Venmo User Agreement. That webpage states that such reviews may result in “funds being frozen or held by Venmo,” “funds being applied to a negative Venmo account balance or used to offset loss incurred by Venmo,” and “account suspension or

termination,” among other consequences. The only reasons offered for taking such drastic and unilateral actions are receiving payment made from a stolen or compromised account or credit card and conducting a “prohibited transaction.” This webpage contains no information about how Defendant conducts these reviews, the criteria used in these reviews, how long a consumer’s money may be held, or how users can recover their funds and/or contest a decision to freeze their accounts.

66. No such language appears in the PayPal user flow, including on the screen allowing consumers to transfer balances to their bank.

67. Neither does Defendant adequately disclose its freeze-and-seize practices on the Venmo and PayPal webpages that claim consumers can freely access and control their account funds. Some of these pages contain no information about Defendant’s freeze-and-seize practices at all.

68. Other webpages contain inconspicuous disclaimers that fail to adequately disclose Defendant’s conduct. On the Venmo “Manage Balance” webpage, for example, several advertising claims—like “[m]ove money from Venmo to your bank account anytime”—are unqualified by disclaimer language. Other claims on this webpage are followed by the same “transfers are reviewed” disclaimer that appears on the transfer balance screen in the Venmo Platform user flow, and likewise fails to adequately disclose the full scope of Defendant’s conduct. A closely similar disclaimer also appears in tiny font at the bottom of this page, in a footnote referenced to Defendant’s description of the Venmo Platform’s direct deposit feature and sandwiched between two disclaimers specific to direct deposits.

69. While Defendant offers some limited additional information in Help Center pages directed at users whose accounts have been frozen, which consumers are unlikely to seek out or

find until after Defendant has frozen their accounts, the only place Defendant describes the full extent of its freeze-and-seize practices is in the Platforms’ lengthy User Agreements.

70. It is well understood that “[g]eneral terms and conditions are often not read, and agreement is typically made automatically and quickly,” providing “an opportunity to fill general terms and conditions with dark ingredients.”⁵ Longstanding industry guidance concerning online disclosures provides that necessary disclosures should not be relegated to terms of use because it is highly unlikely that consumers will read disclosures buried in such documents. Obscuring disclosures in lengthy terms of use is yet another example of the dark design practice of “hid[ing] key information . . . so users will proceed without fully understanding the transaction.”⁶

III. DEFENDANT DECEPTIVELY FAILS TO PROTECT CONSUMERS FROM, OR RESPOND TO, FRAUD ON ITS PLATFORMS.

71. Financial fraud is widespread on e-payment platforms, and PayPal and Venmo are no exception. To reassure consumers that it is safe to send money on its Platforms, Defendant deceptively represents that it protects consumers against losses from fraudulent transactions and acts to assist consumers victimized by fraud. Defendant fails to disclose that, when a consumer falls victim to the pervasive fraud on its Platforms, Defendant does not cover the consumer’s liability for funds lost unless the fraud was of a specific and very narrow type. To qualify as an “unauthorized transaction” against which Defendant offers protection, a criminal must gain unlawful access to and steal funds from the consumer’s account. If the consumer is the one to hit “send” on a Platform transaction, the transaction is not “unauthorized”—even if the consumer was fraudulently induced into sending the lost funds.

⁵ Christoph Bösch et al., *Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns*, Proceedings on Privacy Enhancing Technologies 2016(4), 237, 245 (2016).

⁶ Maximilian Maier and Rikard Harr, *Dark Design Patterns: An End-User Perspective*, 16(2) Human Technology 170, 179 (2020).

72. Third parties unlawfully accessing and stealing from consumers' accounts makes up a fraction of the fraud occurring regularly on the Platforms. Consumers reasonably believe Defendant's advertised fraud protections would naturally include fraudulent transactions in which the consumer is tricked into sending funds to a criminal.

73. Defendant fails to adequately disclose that it will not protect against consumer losses caused by fraud on its Platforms if the consumer initiated the payment, even where the consumer was induced by fraud to make the payment.

74. The only place Defendant explains how it limits consumer protections for fraudulent transactions is in the Venmo and PayPal Platforms' respective User Agreements. A consumer is unlikely to find this language, which appears more than halfway through the 20,000-plus-word legal documents.

75. Even if a consumer did find and read the language, Defendant's explanation of its protections is unclear at best, and at worst, misleading. Under the heading "Protection from Unauthorized Transactions," the agreements state that Defendant "will protect you from unauthorized activity in your [PayPal / Venmo] account," and that Defendant "will cover you for the full amount of the unauthorized activity."

76. Defendant then states that an "unauthorized transaction" occurs when money is sent from your [PayPal / Venmo] account that you did not authorize and that did not benefit you," and provides as an example someone who fraudulently accesses and sends a payment from the consumer's account. Defendant does not explain that fraudulent transactions are considered "authorized," and therefore are not protected, whenever the account holder presses "send" on the transaction—even if the account holder is fraudulently induced into sending the payment.

77. Peer-to-peer payment platforms have fraud rates *three to four times higher* than traditional payment methods like credit and debit cards. According to a study conducted by Javelin Strategy & Research, nearly 18 million Americans were defrauded via digital wallets and person-to-person payment apps in 2020. In a survey of consumers who had used online payment apps, including PayPal and Venmo, 13 percent reported they had sent someone money and later realized it was a scam.

78. This widespread fraud exists on both of Defendant's Platforms. In February 2022, Defendant revealed that it had identified 4.5 million fraudulent PayPal and Venmo accounts. A 2020 New York Times report found that customer reviews of the Venmo Platform mentioning the words "fraud" or "scam" rose 97 percent over the previous year, almost four times faster than its growth in users. Reviews of the PayPal Platform mentioning fraud or scams similarly increased 62 percent over the previous year. PayPal and Venmo's help pages urge consumers to "watch out for" over a dozen "common scams."

79. The COVID-19 pandemic, which prompted consumers to use mobile payment platforms like PayPal and Venmo in record numbers, further accelerated the volume of fraud occurring on these platforms.

80. Defendant is aware of the risk of fraud on its Platforms. In Defendant's own words, "[f]raudulent activities, such as account takeover, identity theft (including stolen financial information), and counterparty malicious activities, represent a significant risk to merchants and consumers, as well as their payment partners."

81. To reassure consumers that its Platforms are safe to use, Defendant advertises that it protects consumers' PayPal and Venmo accounts from fraud and assists consumers in the event they fall victim to fraudsters.

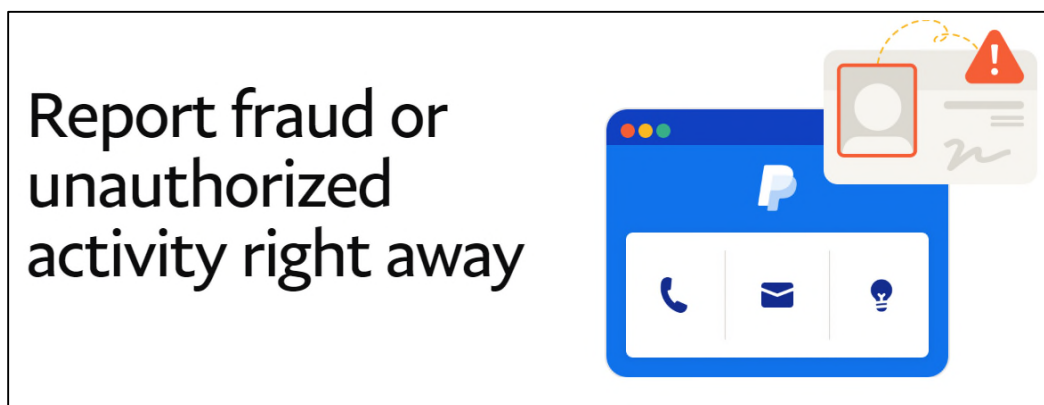
82. On the PayPal website, Defendant assures consumers that its “advanced fraud detection technology” helps “protect your account from fraudulent charges.”

83. On the Venmo website, Defendant similarly promises consumers that it “help[s] protect your transactions with PayPal’s trusted monitoring and encryption technology.”

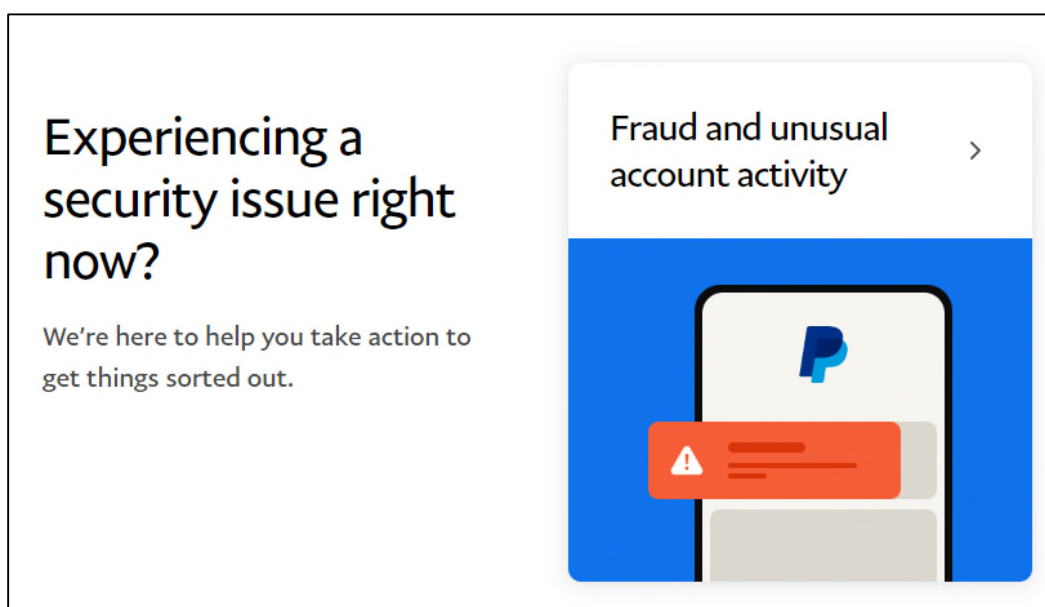
84. A Venmo help page further represents that Defendant “monitor[s] your account activity to help identify unauthorized transactions.”

85. In a statement to CNBC, Defendant touted its so-called advanced fraud protection measures, stating they included “enhanced transaction monitoring to detect unusual patterns in payments moving through our platforms,” “key word tracking, suspicious matter reporting, sanctions and watch list enforcement, and other sophisticated fraud detection models to protect our customers.”

86. Defendant also warns consumers that it is “extremely important” to report unauthorized transactions to Defendant so that Defendant can investigate and “take the necessary steps to secure your account,” which would lead a reasonable consumer to believe that Defendant protects account holders who are victimized by fraud on its Platforms against the loss of their funds.



87. Defendant’s security webpages are also replete with misrepresentations that its customer support will assist consumers with security issues, further conveying that Defendant will protect consumers victimized by fraud against losses. On the PayPal “Security Center” webpage, under the heading “Your security is our priority,” Defendant promises that “[w]e’re here to help you take action to get things sorted out.” On its Safety and Security webpage, under the heading “Fraud prevention,” Defendant similarly prompts consumers to “[c]ontact us if anything seems suspicious so we can help you protect yourself from fraudulent charges against your account.”



88. On Venmo’s “trust and safety” webpage, Defendant promises that “Venmo has your back” and that “[o]ur support team is here for you.” A Venmo help page concerning account security similarly tells consumers that Defendant’s “[s]ecurity support” is “here to help.”

89. These unqualified representations reinforce consumers’ existing expectation that financial services companies like Defendant will help them recover funds sent in error—whether caused by a simple mistake or fraud. In one national survey, more than half of consumers believed—incorrectly—that mobile payment companies like Defendant would return or reimburse money sent in error.

90. Defendant's claims deceptively convey to consumers that Defendant protects consumers against losses caused by fraudulent transactions. These statements are misleading because they do not disclose that Defendant's fraud protections are exceedingly limited and do not cover the pervasive fraudulent schemes that trick consumers into sending money to the fraudster.

91. In one example, a Hawai'i consumer reported being scammed by criminals posing as a company with which the consumer had an existing subscription. The criminals' email to the victim accurately stated that the consumer's subscription was expiring soon and directed the consumer to use PayPal to renew the subscription. After the consumer sent the payment via PayPal, they discovered that the email was fraudulent. Despite contacting PayPal immediately to report the fraud, PayPal informed the consumer that PayPal would not do anything to help and, unbelievably, that the consumer would have to resolve the issue directly with the criminals who had defrauded them.

92. In another example, a Hawai'i consumer used PayPal to pay for what they believed was a home rental. The scammers instructed the consumer to send \$3,100 via PayPal and promised to reimburse the consumer if they were not satisfied with the property. After the consumer sent the payment, they discovered that the rental listing was a scam. Defendant informed the consumer that it would not refund the payment.

93. Defendant's refusal to provide any recourse for consumers victimized by this type of rampant fraud is material to consumers, costing them significantly in both money and time spent trying to get help from Defendant to recover their funds. In 2021, the Better Business Bureau

reported that the median dollar loss for online purchase scams on Venmo was approximately \$700—the second highest such loss amongst all payment services.⁷

IV. DEFENDANT’S PURCHASE PROTECTION PROGRAMS DECEIVE CONSUMERS AND UNFAIRLY ASSESS FEES WITHOUT NOTICE.

94. Defendant has further attempted to reassure consumers, who are rightfully concerned about the rampant fraud on its Platforms, with “Purchase Protection” programs. The Purchase Protection programs on the PayPal and Venmo Platforms purport to apply to transactions for goods and services.

95. Defendant has offered Purchase Protection on PayPal since 2003, and it launched Venmo’s version of the program in July 2021.

96. PayPal executives have boasted publicly that the purpose of the programs is to provide an added layer of protection to users transacting on its Platforms. As PayPal’s then-Executive VP & COO, William Ready, informed investors, “[w]e offer buyer protection. We offer seller protection, solving for the fraud around these things. Other players aren’t solving that, so it’s not just that we bring a seamless transaction. It’s that we’re guaranteeing both sides of that transaction[.]”

97. However, like its so-called fraud protection, Defendant’s “Purchase Protection” is significantly narrower than what consumers are led to believe. On the Venmo Platform, Defendant deceptively represents that consumers who “turn on” Purchase Protection for goods and services transactions receive a full refund if something goes wrong with their purchase. In fact, Purchase

⁷ Online purchase scams are scams that involve the purchase of products or services online. Scammers typically offer attractive deals or advertise hard-to-find goods, but when payment is made, do not deliver the purchase product or service.

Protection only applies to a narrow subset of such transactions, and the only thing guaranteed to consumers who opt in is the ability to apply for a refund.

98. At the same time, Defendant unfairly charges consumers on the receiving side of the transaction a fee—even when the transaction is not for goods and services—if the consumer sending the funds opts into the Purchase Protection program. On Venmo, this fee is calculated as 1.9 percent of the payment plus \$0.10.⁸ On PayPal, the fee is 2.99 percent of the transaction. Defendant deducts this fee from the funds sent to the recipient.

99. In the classic example of friends splitting their restaurant tab, if the friend sending money shifted the toggle to “protect” the transaction, Defendant would deduct a Purchase Protection fee from the amount ultimately delivered to the recipient even though this transaction does not qualify for protection. In these instances, Purchase Protection is entirely illusory, and Defendant is collecting fees for a protection it does not offer. Making matters even worse, Defendant offers no way for consumers who are incorrectly charged a Purchase Protection fee to reverse it.

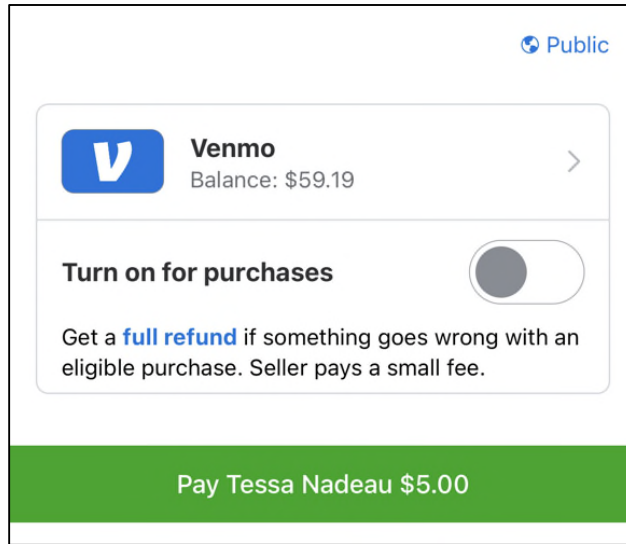
A. Defendant Deceptively Promises Venmo Users Full Refunds When They “Turn On” Purchase Protection.

100. Since July 20, 2021, Defendant has offered consumers on Venmo the ability to “turn on” a feature that Defendant deceptively represents will allow consumers to “[g]et a full refund if something goes wrong with an eligible purchase” or “if an eligible purchase isn’t what you paid for.” Defendant also informs consumers that the “Seller pays a small fee.”⁹

⁸ When a consumer sends money to a PayPal or Venmo business account, rather than a personal account, Defendant’s Purchase Protection programs apply automatically.

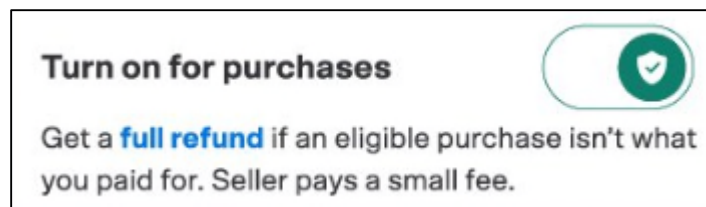
⁹ In the context of Defendant’s Purchase Protection program, “Seller” refers to the recipient of the funds.

101. Defendant deceptively presents the feature as a switch that consumers can toggle on and off. The toggle switch appears immediately above the “Send” or “Pay” button, just before the user completes a transaction.



102. In the mobile app, if a Venmo user clicks on the linked term “full refund,” a pop-up screen appears. Titled “Full refund on eligible purchases,” the pop-up tells consumers that when they “[t]urn on” Purchase Protection, “you’ll get your money back in cases where an eligible purchase is” not as described, damaged, or not received. On the web, the linked term “full refund” links to the webpage advertising the Venmo Purchase Protection program, which deceptively tells consumers that Purchase Protection is “available when you tell Venmo you’re paying for a good or service before you send a payment in the app.”

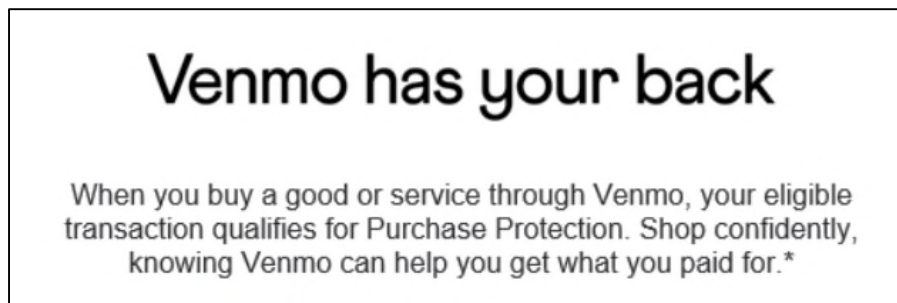
103. When toggled on, the toggle switch appears as a green button containing a shield with a checkmark on it.



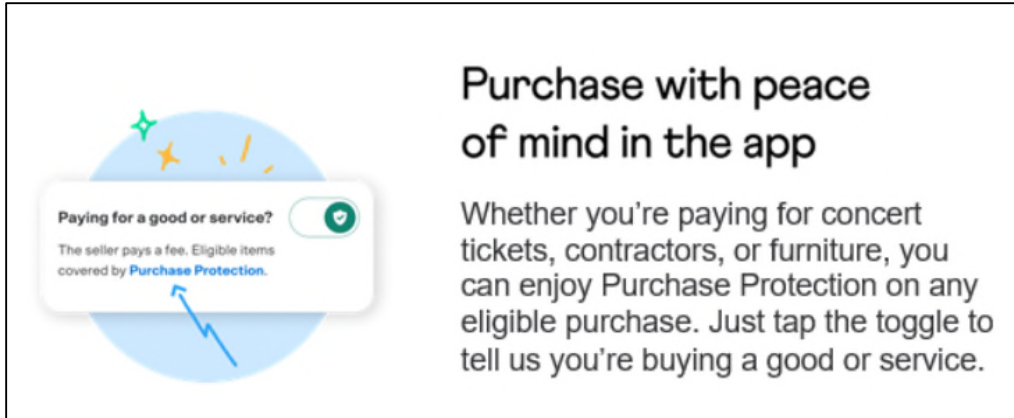
104. In the Venmo mobile app, after the switch is toggled on, a pop-up screen appears. This pop-up similarly tells consumers that “[t]urning on” the feature “for purchases” means that the consumer “will be covered by Purchase Protection on eligible transactions.”

105. At no point in the Venmo user flow does Defendant explain which purchases of goods and services are “eligible” for its Purchase Protection program.

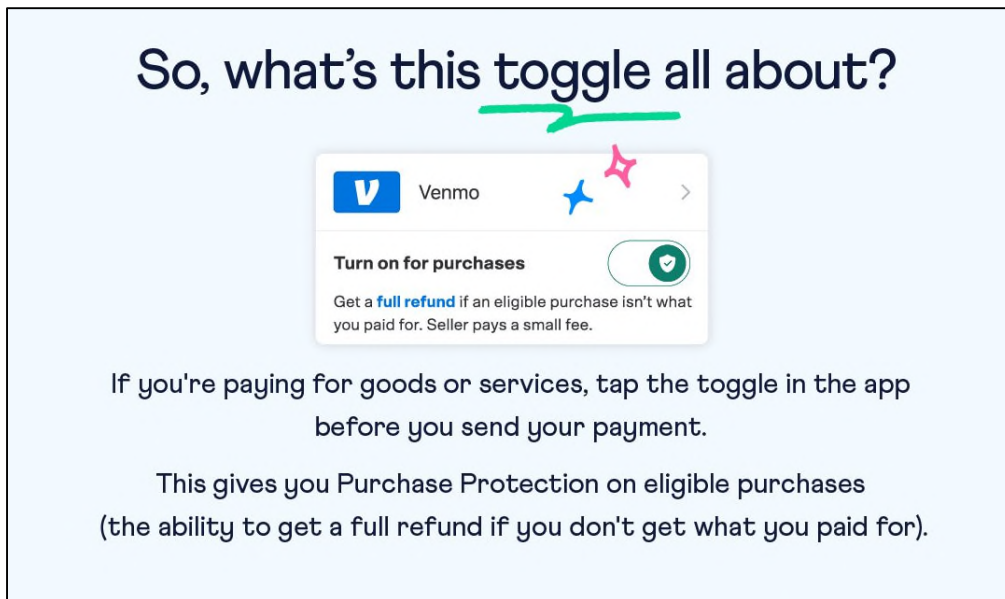
106. In a December 2021 email sent to Venmo users advertising the Purchase Protection program, Defendant represented that consumers receive Purchase Protection on transactions for goods and services. The email, which, on information and belief, was sent to every Venmo user, including Venmo users in Hawai‘i, stated, “[w]hen you buy a good or service through Venmo, your eligible transaction qualifies for Purchase Protection.”



107. Further reinforcing that Defendant’s program offers broad protection for goods and services transactions at the click of a button, the email further stated, “Whether you’re paying for concert tickets, contractors, or furniture, you can enjoy Purchase Protection on any eligible purchase. Just tap the toggle to tell us you’re buying a good or service.”



108. Defendant similarly represented that tapping the toggle button “gives you Purchase Protection” in a Twitter post that asked “So, what’s this toggle all about?”



109. Defendant’s representations about the Venmo Purchase Protection program, and its presentation of the Purchase Protection program in the Venmo user transaction flow, deceptively convey to consumers that all transactions for the purchase of goods and services are eligible for Purchase Protection, and that simply “turning on” the toggle switch for such transactions entitles the consumer to a “full refund” if something goes wrong. In reality, Purchase Protection only covers certain goods and services transactions, and toggling it on does not guarantee the user a refund if something goes wrong.

110. Buried almost halfway through the more than 20,000-word Venmo User Agreement is a list of 16 broad categories of goods and services transactions that are excluded from its Purchase Protection program altogether, including:

- Payments for goods that the buyer “collects in person or arranges to be collected on their behalf” (rather than having the goods shipped);
- “Vehicles, including, but not limited to, motor vehicles, motorcycles, recreational vehicles, aircraft and boats”;
- Payments for “stored value items such as gift cards and pre-paid cards”;
- “Financial products or investments of any kind”; and
- “Anything Venmo determines, in its sole discretion, is prohibited by this user agreement and/or the Acceptable Use Policy, even if the transaction is initially marked as ‘Purchase Protected’ on the transaction details page.”

111. To fully understand the scope of the exclusions, a consumer also would have to review the entirety of the User Agreement along with the incredibly broad Acceptable Use Policy discussed previously.

112. These hidden—and unexpectedly broad—exclusions leave Hawai‘i consumers holding the bag when they learn their transactions are not protected despite having clicked the Purchase Protection toggle. In one example, a Hawai‘i consumer clicked on the Purchase Protection option to cover the purchase of stock from a person on Instagram promising big returns. The consumer sent \$800 through Venmo before realizing it was a scam. When the consumer filed a dispute, Defendant refused to issue a refund.

113. Even if a consumer’s goods and services transaction is not officially excluded from the program, opting into Purchase Protection does not mean the consumer will actually “get a full refund if something goes wrong.” Purchase Protection merely allows the consumer to submit a claim for a refund.

114. Defendant subjects such claims to a myriad of conditions disclosed only in its Venmo User Agreement, and it retains “sole discretion” to determine “whether the claim is eligible for the Venmo Purchase Protection Program.” These conditions include requiring users to have attempted to resolve the issue with the seller and to submit a claim within 180 days of the purchase.

115. Defendant’s representations that a transaction is covered by Purchase Protection and that consumers will receive “a full refund if something goes wrong,” are material to consumers when deciding whether to pay with Venmo or to use alternate forms of payment with robust consumer protections, like credit cards.

116. Defendant does not provide adequate notice that “turning on” Purchase Protection does not mean a transaction for goods and services qualifies for protection. As shown above, Defendant’s original presentations of the toggle button in the Venmo user transaction flow did not include a link to the applicable terms.

117. Currently, the words “Terms apply” appear in small font outside of the box prompting consumers to “turn on” Purchase Protection. The words link to the Venmo User Agreement.

118. Hyperlinking to the lengthy Venmo User Agreement, in which the key terms of the Purchase Protection program are buried, is wholly inadequate to correct the net impression resulting from Defendant’s express misrepresentations. As alleged in Section II.C, *supra*, it is highly unlikely that consumers will read disclosures buried in terms of use. In fact, longstanding industry guidance on online disclosures advises companies that hyperlinks are inadequate to communicate “disclosures that are an integral part of a claim. It further provides that, where a hyperlink is appropriate and necessary due to the complexity of the information, it should be clearly labeled to alert the consumer to the specific nature of the information to which it leads.

B. Defendant Unfairly Charges Consumers a Purchase Protection Fee for Transactions that Do Not Qualify for Purchase Protection.

119. Contrary to a spokesperson's statement that the "buyer and seller safeguards" associated with Defendant's Purchase Protection programs "are completely voluntary," recipients of funds have no control over when the program—and associated fee—is applied to their transactions. Defendant unfairly allows this fee to be triggered even when a transaction does not qualify for Purchase Protection. In those circumstances, Defendant keeps the fee and provides consumers with no recourse to challenge the imposition of the fee.

120. On both the Venmo and PayPal Platforms, Defendant's Purchase Protection programs rely on consumers to identify when the payment they are sending qualifies for Purchase Protection. When a consumer chooses this option when making a payment, Defendant automatically charges the recipient of the payment a fee.

121. Defendant permits the consumer sending the payment to trigger this Purchase Protection fee even when the transaction is not for goods or services, and therefore does not qualify for Purchase Protection under the terms of the programs—for example, when splitting the cost of a meal between friends.

122. Defendant does not notify the payment recipient that a fee will be subtracted from the funds they receive until the transaction is completed and the fee is charged.

123. On information and belief, Defendant knows or should know that some Venmo and PayPal Platform transactions that consumers identify as for goods or services are not, in fact, for goods or services, or otherwise do not qualify for Purchase Protection under Defendant's own terms. Defendant's assessment of these fees, in violation of the terms of its own Purchase Protection programs, violates the duty of good faith and fair dealing implied in every contract.

124. In one example posted to PayPal’s Community Forum, a PayPal user reported that, after having received her monthly child support payments via PayPal for six months without incident, PayPal began listing the user as a “seller” and her ex-husband as a “buyer,” after which “\$17 was taken out” and placed on “hold” until the user proved that the “shipment” had been received.

125. Defendant does not provide any mechanism for a payment recipient to reverse the Purchase Protection fee—even when the sender selected the Purchase Protection option accidentally, or when the transaction is not a payment for eligible goods or services.

126. On the Venmo Platform, Defendant merely directs payment recipients to ask the sender to contact Venmo customer support. There is no way for a payment recipient to appeal the fee on his or her own.

127. On the PayPal Platform, Defendant provides no instructions at all on how payment recipients can reverse Purchase Protection fees charged on non-qualifying transactions.

128. One Hawai‘i consumer reported that they were charged a nearly \$30 fee for a transfer from a friend on the PayPal Platform. The consumer reported that the friend had not selected the “goods and services” option, but Defendant nevertheless withheld the fee from the funds the friend sent the consumer. PayPal support offered no way to recover the fee, leaving the consumer feeling “ripped off.”

129. Another Hawai‘i consumer reported that Defendant refused to refund a \$12.19 Purchase Protection fee charged when the consumer’s sister accidentally sent her money marked as for goods or services. Repeated calls to customer support were unsuccessful, and the consumer received only automated responses to her emails.

130. The aggregate consumer injuries caused by Defendant's incorrectly and unilaterally charged Purchase Protection fees, for an illusory protection that was never provided, are substantial.

131. At no point does Defendant notify consumers that they may be charged a Purchase Protection fee without notice on transactions that do not qualify for Purchase Protection, or that consumers charged such fees have no way to directly appeal a wrongfully imposed fee.

V. DEFENDANT DECEPTIVELY AND UNFAIRLY VIOLATES CONSUMER PRIVACY AND FACILITATES FRAUD BY MAKING VENMO ACCOUNT INFORMATION PUBLIC.

132. The Venmo Platform's very design deceptively and unfairly violates consumer privacy. Its default privacy settings make public consumers' personally identifiable financial information, contradicting Defendant's express representations about consumer privacy on the Platform, violating consumers' privacy rights and expectations, and exposing consumers to fraud. This practice sets Venmo apart from its industry competitors: no other peer-to-peer payments service exposes its users' personally identifiable financial information in this way.

133. Defendant makes consumers' Venmo information public as a deliberate business strategy to drive growth. PayPal CEO Dan Schulman has called Venmo's social experience, which Defendant creates by publicizing users' Venmo activity in user feeds and user profiles, its "secret sauce."

134. Venmo is a "closed system"—Venmo users can only transact with other Venmo users. As such, growing the platform's user base is integral to its success. To convince people to use the service, Defendant exploited the concept of "social proof," the phenomenon in which individuals look to their peers to inform their own decisions and actions. As explained by a Venmo product lead, publicizing Venmo users' information was "really important" to convincing consumers to use the service because it allowed consumers to see that their friends and many others

were using it, validating that the service was both useful and trustworthy. A former Venmo engineer similarly explained that using consumers' social networks made it easier to instill the trust necessary to agree to send or receive money with the service.

135. At the same time, consumers expect their financial information to be kept private. In attempting to reconcile these irreconcilable demands—protecting personal financial information on a “social payments” platform—Defendant engages in several deceptive and unfair practices.

136. First, Defendant deceptively represents that consumers' financial information on Venmo is kept private, reinforcing what a reasonable consumer would believe based on financial industry norms. However, Defendant publishes consumers' personally identifiable account information, transactions, and contact lists by default, and in some cases, does not allow consumers the option to keep this information private. Second, Defendant misrepresents the limited purposes for which it uses the personally identifiable account and contacts information that it prompts consumers to provide when signing up with Venmo. Third, Defendant failed to disclose that it was broadcasting detailed Venmo transaction data—again containing personally identifiable financial information—via a freely accessible software tool that allowed anyone on the Internet to access, download, and exploit this sensitive data in bulk. Defendant's publication of this sensitive financial information unfairly renders consumers vulnerable to the rampant fraud on its Platforms. Finally, Defendant's privacy setting for past transactions misrepresents to consumers that they can limit the audience for transactions that Defendant already published, both on and off its Platform.

A. Defendant Deceptively Promises Venmo Users Privacy While Making Their Financial Information Public by Default.

137. Defendant’s representations about Venmo’s services, and the nature of Venmo’s services themselves, deceptively convey to consumers that Defendant is a financial services provider that will keep Venmo users’ personal financial information private.¹⁰

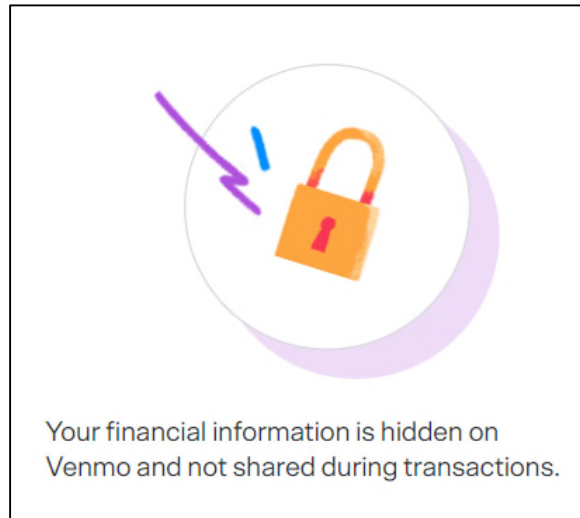
138. The services Defendant provides on the Venmo Platform are financial services. Venmo is classified as a “finance” app in the Apple App Store and in Google Play, and its Facebook profile lists it as a “Financial Service.” Defendant describes Venmo as a “way to pay and get paid,” and prominently includes “send and receive money” and “manage your money” in descriptions of its services. In an interview, a Venmo product lead described Venmo as “first and foremost a payments app,” and recognized that consumers had the same understanding: “people really do view Venmo first and foremost as a payments app.”

139. Defendant expressly tells consumers that, “[a]s a global payments company, one of our greatest responsibilities is to ensure the appropriate use and protection of our customers’ personal data and financial information.” It further represents that it employs a “privacy-first approach” to its use and protection of customer data.

140. Defendant also expressly advertises that “[y]our financial information is hidden on Venmo and not shared during transactions,” allowing consumers to “[s]end dollars, not financial details.” It represents that “[e]very transaction in our app is encrypted, so your financial

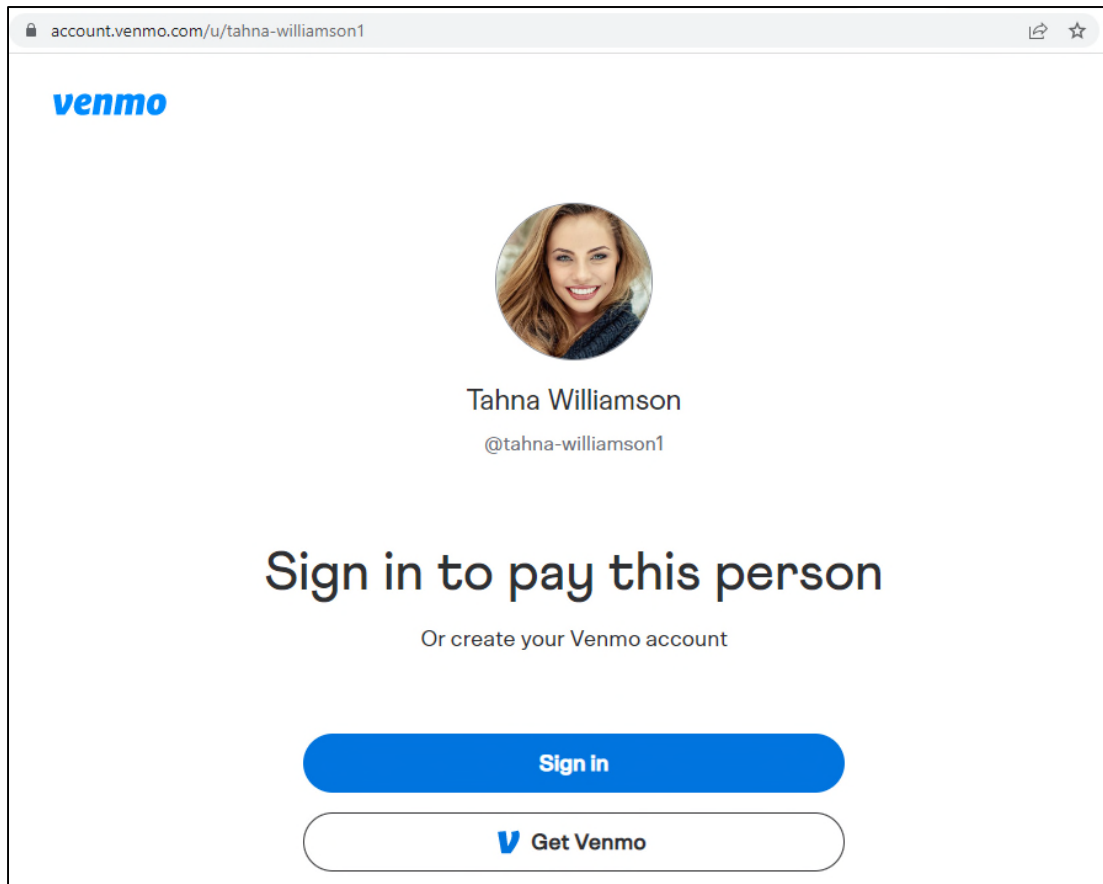
¹⁰ Personally identifiable financial information includes any information a consumer provides to a financial institution to obtain a financial product or service. It also includes information about a consumer related to a financial transaction. Examples include the fact that a consumer is or was the customer of a particular financial institution, account information, payment history, and purchase information, among others.

information stays secure,” and that when consumers use Venmo to pay for transactions on other apps or shopping at online retailers, “we’ll send the payment without sharing your account details.”



141. Contrary to these representations, Defendant publicizes Venmo users’ personally identifiable financial information unless consumers take affirmative steps to keep it private. And Defendant does not allow consumers to keep certain Venmo account information private at all.

142. Defendant creates and maintains a publicly accessible webpage for every Venmo user account that displays the consumer's name, Venmo user name, and profile photo. Consumers have no ability to keep this information private.



143. Defendant does not allow Venmo users to delete profile photos—once a consumer has uploaded a photo, the only way to remove it is to upload another. Until at least May 2021, consumers' previously-used profile photos remained publicly accessible on Venmo's website.

144. This practice can have serious privacy consequences. One Hawai'i consumer reported a photograph of the consumer's 5-year-old child had been used as an unknown person's Venmo profile picture. When the consumer called to report the issue and ask that the photograph be removed, Venmo support said the photograph could not be removed and hung up. In the words

of the distressed consumer, “how do I protect my child? She could be the face of sex trafficking now, I DON’T KNOW THIS PERSON, IT’S NOT SAFE.”

145. Defendant’s practice of publishing this personally identifiable information reveals, to everyone on the Internet, that a specific, identifiable consumer has a financial account with Venmo, the consumer’s user name for that account, and frequently, what the consumer looks like. This is the sort of user information published by social media platforms like Facebook and Twitter, not financial institutions—and even those social media platforms offer privacy settings that allow users to prevent others from searching for their accounts. Venmo does not.

146. Defendant also makes Venmo users’ friends lists public by default, exposing consumers’ social and financial networks to the nearly 90 million people on Venmo. Venmo friends lists appear in consumers’ Venmo profiles, and may include the consumer’s entire catalog of mobile phone contacts and Facebook friends, as discussed further in Section V.B, *infra*.

147. Venmo allows users to collect others’ friends information in bulk: according to a recently published academic study, logged-in Venmo users can crawl the platform to build a list of contacts for any user whose friends list is publicly visible.

148. Venmo friends lists were also accessible to non-Venmo users until at least May 2018. One programmer was able to quickly collect the friends lists of a million Venmo users and analyze their social networks with open-source code that scraped user data using dummy Venmo accounts.

149. Defendant did not offer Venmo users the ability to keep their friends lists private until in or around June 2021. Before that time, the only way Venmo users could protect their friends lists from public exposure was to manually remove each person from their friends list one-by-one.

150. Just as it does for Venmo users' names, user account names, profile pictures, and friends lists, Defendant also makes Venmo users' transactions public by default. Defendant makes all transactions public unless the consumer affirmatively acts to limit the audience for the transaction.

151. For every public Venmo transaction, Defendant publishes the user names of the parties to the transaction, the profile photo of the user initiating the transaction, and the description of the transaction entered by the user initiating the transaction. Defendant requires consumers to enter a description in order to send or request a payment.

152. Defendant publishes public transactions in Venmo users' profiles, which are accessible to any Venmo user. Additionally, until July 2021, Defendant also published public transactions to all signed-in Venmo users in the "global view" of the Venmo user feed (similar to Facebook's "News Feed"). Defendant populated this feed with other Venmo users' transactions, regardless of whether the other users had any relationship with the consumer viewing the feed.

153. Defendant's publication of consumers' personally identifiable Venmo account and transaction information is material to consumers. This financial information is highly sensitive. The Hawai'i Supreme Court has recognized that "financial transactions can reveal much about a person's activities, associations, and beliefs." The Electronic Frontier Foundation has similarly warned that "[t]he list of people with whom you exchange money paints a startlingly clear picture of the people who live, date, and do business with you." Publicizing this information exposes consumers to the risk of harassment and fraud, in addition to personal embarrassment.

154. Consumers reasonably expect this kind of sensitive financial information to be private. One survey found that 56 percent of consumers consider the unauthorized sharing of financial information to be their primary privacy concern, which is more than double the

percentage of consumers who rated sharing health information as their primary concern. For nearly two-thirds of consumers, “privacy is always top of mind whenever they interact with their financial services institution.” And 83 percent wanted the opportunity to opt out of sharing of information with financial institutions.

155. These reasonable consumer expectations are reinforced in a variety of state and federal laws, including the Hawai‘i Constitution, which specifically protects “the right to keep confidential information which is highly personal and intimate”—including financial records.

B. Defendant Deceptively Claims That Venmo Users’ Account and Contacts Information Is Used for Limited Purposes.

156. Defendant deceptively represents to consumers that their personally identifiable Venmo account information will be used for limited purposes, but fails to adequately disclose that Defendant publishes this information to everyone on the Internet.

157. Defendant requires consumers to enter their legal names when signing up for Venmo, and automatically associates this name with the consumer’s user name and profile photo. Defendant represents to consumers that it “collect[s] your legal name when you sign up so you can get a head start on the identity verification process,” which Defendant states is “required” by “federal law,” and that identity verification “is primarily what this information is used for.”

158. Even before Defendant expressly required consumers to enter their legal names at sign-up, consumers on Venmo frequently used their real names when creating their accounts. Defendant encouraged this practice, prompting consumers to use their real names when creating a user name with the language “Help people know it’s you they’re paying.” Defendant also prompted consumers to add a profile picture using the same language, conveying that consumers should use personally identifiable photographs in their Venmo profiles.

159. These statements convey that Defendant uses the personally identifiable information it prompts consumers to provide when creating their accounts for limited purposes: facilitating the consumer's use of the Venmo Platform and fulfilling legal requirements to verify the consumer's identity. However, as discussed in Section V.A, *supra*, Defendant publishes Venmo users' names, user names, and profile photos on publicly accessible webpages and does not allow consumers to keep this personally identifiable account information private.

160. During sign-up, Defendant encourages consumers to sync their mobile phone contacts with their Venmo accounts to "make it easier to find and pay your friends. It also helps to protect your Venmo account." Until recently, Defendant also prompted consumers to sync their Facebook profiles with their Venmo accounts, with language that doing so would allow users to "easily find, pay, and share payments with each other."

161. In the "Friends & Social" section of Venmo's account settings, Defendant similarly described the purpose of allowing Venmo to access the consumer's Facebook friends as allowing the consumer to "easily find and pay them, and they can share payments with you."

162. These representations convey that Defendant uses consumers' mobile phone contacts and Facebook friends for a limited purpose: to facilitate the consumer's use of the Venmo Platform by allowing the consumer and the consumer's contacts to find one another more easily on Venmo. Defendant fails to inform consumers that it also makes consumers' Venmo friends lists available to everyone on the Platform.

163. Complying with Defendant's prompts to sync the consumer's contacts and Facebook account with their Venmo account allows Defendant to access the names, phone numbers, and email addresses stored in the consumer's mobile phone, along with the consumer's Facebook profile and Facebook friends list. Defendant uses this information to identify the

consumer's contacts and Facebook friends that are Venmo users and add those users to the consumer's public Venmo friends list. Defendant accesses this information and updates users' Venmo friends lists on an ongoing basis.

164. These practices are material to consumers. A consumer's Venmo friends list can expose highly sensitive information. For example, therapists and mental health professionals that accept payment through Venmo risk publicly exposing the identity of their clients; similarly, patients risk publicly exposing the fact that they are receiving mental healthcare and the identity of their providers.

165. Defendant's publication of consumers' Venmo account information has also exposed consumers to harassment. In one complaint posted on PayPal's community webpage, a consumer reported being harassed by a person they did not know with repeated payment requests that included "horrible foul language."

166. In addition to the privacy concerns raised by Defendant's sharing of consumers' personally identifiable financial account information, publishing this information renders consumers vulnerable to fraud.

167. Consumers' Venmo account and friends information has been widely used in social engineering attacks to defraud users. In these schemes, a bad actor identifies a consumer's publicly available Venmo account, uses the consumer's public friends list to create a Venmo account that appears to be a person the consumer knows, and poses as that person to request money on the Platform. Scammers also use the same technique in reverse, creating Venmo accounts that appear to be a consumer's account and sending requests to everyone on the consumer's Venmo friends list.

168. In one example, a Hawai'i consumer was scammed by a fraudulent account mimicking their daughter's account. The fraudulent account requested \$300, and mistakenly believing the account to be their daughter's, and the consumer paid it, realizing only afterward that they had been scammed. The consumer reported that Venmo support provided no help to resolve the issue or recover the money—and to add insult to injury, said the loss was the consumer's fault.

169. Defendant has known about these vulnerabilities for years: as early as 2014, academic researchers detailed how Venmo's user interface design rendered consumers on the platform vulnerable to fraudulent requests for payment. In 2015, the national publication *Slate* reported that, "since Venmo users can quickly change things like their name and profile picture, it's easy for hackers to impersonate users' actual contacts and trick them into sending money to the wrong accounts."

170. Defendant's own help page detailing "common scams on Venmo" includes a scam in which "Someone Pretends To Be Your Friend And Requests Money." The description notes that "[u]sing information visible in the public feed," scammers "may change their username and profile picture to impersonate someone you may know" in order to request money. The description also states that consumers can "[u]pdate the privacy settings" on Venmo, further acknowledging that its default privacy settings render consumers vulnerable to such fraud.

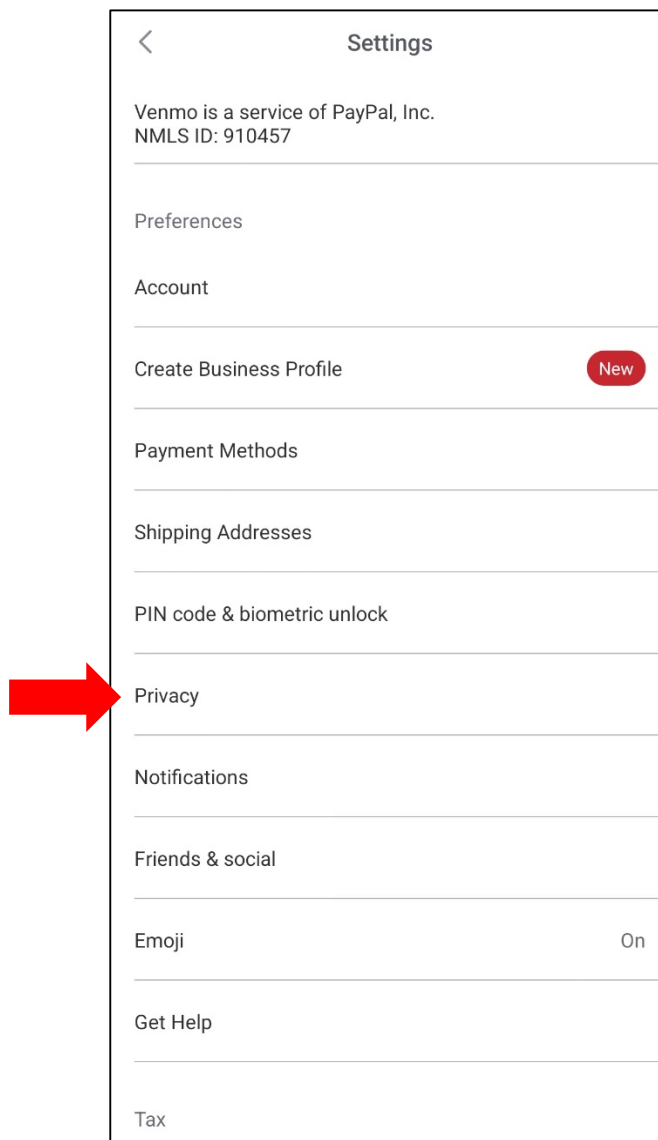
171. Defendant has not addressed these longstanding vulnerabilities. Venmo users can still change their name, user name, and the photograph associated with their accounts at will. And Defendant does not verify the identities of Venmo account holders before allowing them to request and receive money.

172. Despite its knowledge of these significant privacy and fraud concerns, Defendant only began allowing consumers the option to make their Venmo friends lists private after causing

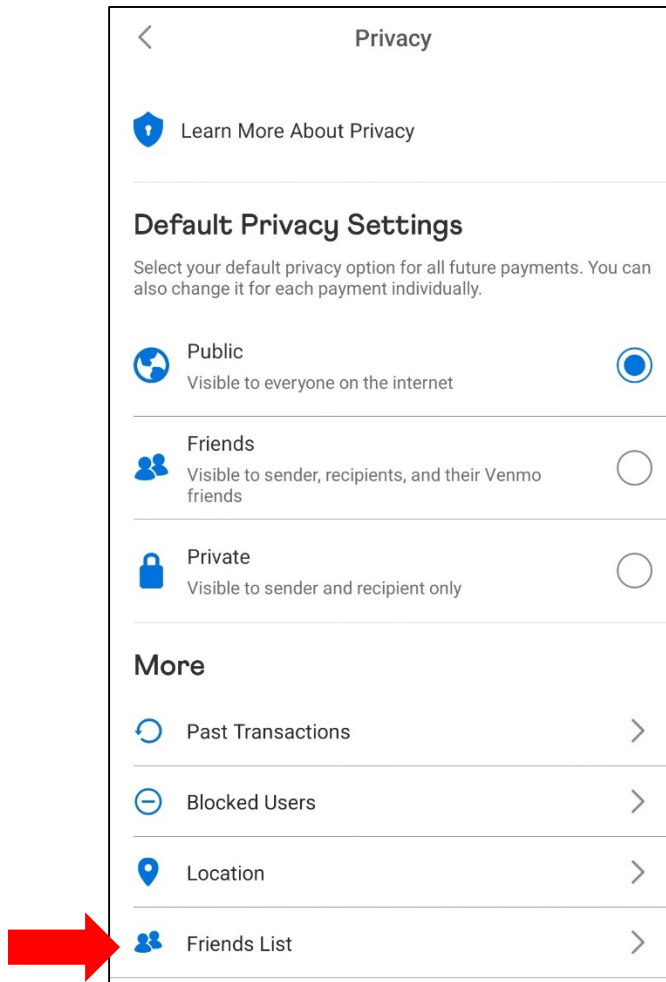
a minor national security crisis. Journalists reported they were able to easily find President Biden’s Venmo account, and through it, identify the Venmo accounts of Biden family members and senior White House officials.

173. Even now, as discussed in Section V.A, *supra*, Venmo friends lists remain public by default. To make their Venmo friends lists private, consumers must:

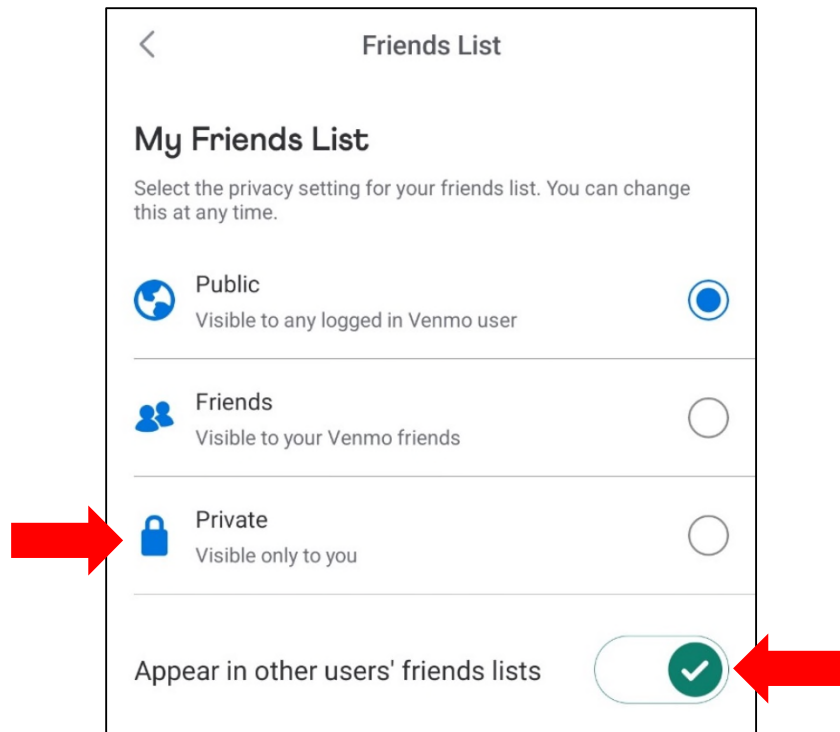
- a. Navigate to the Settings menu;
- b. In the Settings menu, click on Privacy;



- c. On the Privacy screen, click on “Friends List,” which appears at the bottom of the screen and requires scrolling past three radio buttons offering choices for “Default Privacy Settings”; and



- d. On the Friends List screen, select “Private” as “the privacy setting for your friends list” and toggle off a separate setting to avoid appearing in other users’ friends lists.



174. This process is not intuitive for the average consumer.

175. Industry guidance on consumer privacy practices has made clear that consumers should not have to navigate through multiple screens to find privacy settings. Yet, this is precisely what Defendant requires consumers to do to make their friends lists private. Worse, to reach the “Friends List” privacy settings, Defendant requires consumers to navigate past a separate, more prominent set of “Default Privacy Settings.”

176. Defendant does not provide notices or prompts related to the privacy of friends lists in its mobile account sign-up process for new users. On information and belief, Defendant did not issue any in-app notice to existing Venmo users when it added the new privacy feature for friends lists in mid-2021. Absent effective notice of these new privacy options, consumers are unlikely to use them.

177. The only measure that Defendant has implemented to prevent consumers on Venmo from sending money to fraudsters weaponizing consumers’ public Venmo account information is

a single pop-up screen that prompts consumers to enter the last four digits of the recipient's phone number before sending a payment to an account that is not in the consumer's contacts. This pop-up appears only in the Venmo mobile app, not on the Venmo website where consumers also transact.

178. Defendant does not require consumers to enter this information before sending a Venmo payment. In fact, a button allowing consumers to "Pay Without Confirming" appears more prominently in the pop-up than the "Confirm" button, which remains grayed out unless the consumer enters the last four digits of the recipient's phone number.

179. This pop-up also does nothing to mitigate scams in which fraudsters take advantage of public Venmo account information to target consumers using tactics other than impersonating a person the consumer knows, including online purchase scams, scams in which fraudsters purport to send consumers money on Venmo and ask for it back, and fake charity scams, among many others.

180. Further, the warning that appears in this pop-up is itself misleading. This warning states: "Keep in mind, there's no guarantee you'll get your money back if someone scams you." In fact, as discussed in Section III, *infra*, Defendant provides no protection or recourse for recovering funds when consumers are scammed on Venmo, and as a result, it is practically certain that consumers will *not* get their money back.

181. Defendant does not adequately disclose that consumers' personally identifiable Venmo account information is publicly available, and that Defendant offers consumers no option to keep certain personal financial information private.

182. The current sign-up screen prompting consumers to sync their phone contacts contains no disclaimers. A previous version of the Venmo mobile app represented that Defendant

would use the shared contacts data “to friend those that use Venmo, help you invite those that don’t, improve your search results and as noted in our Privacy Policy.” The Privacy Policy was not hyperlinked. This language reinforced Defendant’s misleading representations that Venmo friends lists are used to facilitate the consumer’s Venmo transactions. The sign-up screen prompting users to connect their Facebook accounts did not reference the Privacy Policy at all.

183. Prior to September 2018, the Venmo Privacy Policy included no language concerning the public availability of consumers’ Venmo account information and friends lists.

184. Beginning in September 2018, Defendant added language to the Venmo Privacy Policy stating that a Venmo user’s user name, profile photo, and first and last name “is public information” that may be seen by anyone on the Internet. It did not disclose that consumers who use Venmo have no option to keep this information private. It also stated that “your Venmo friends list may be seen by any logged-in Venmo user,” failing to disclose that consumers had no option to keep this information private until in or around June 2021, or that it was possible for non-Venmo users to access consumers’ Venmo friends lists. This language appears more than halfway through the 3,000-plus-word Privacy Policy.

185. Consumers are unlikely to see this language. As discussed in Section II.C, *supra*, necessary disclosures should not be relegated to terms of use because it is highly unlikely that consumers will read such disclosures. Further, given their expectations about the privacy of financial information, *see supra* Section V.A, consumers would not think it necessary to read a lengthy legal document to confirm that their personally identifiable financial account information would be kept private.

186. These practices prevent consumers from being able to reasonably avoid sharing sensitive personal financial account information without their knowledge, increasing their vulnerability to fraud and harassment, among other harms.

C. Defendant Deceptively Failed to Disclose that It Broadcast Venmo Users' Personally Identifiable Transaction Data via a Public API.

187. Defendant's default privacy settings make public all transactions on the Venmo Platform, as alleged in Section V.A, *supra*.

188. Until approximately mid-2021 to early 2022, Defendant allowed not just Venmo users, but anyone on the Internet, to access consumers' Venmo transaction data through an application programming interface ("API"),¹¹ which Defendant allowed anyone to use without authentication. The Venmo API was effectively a freely available, real-time data feed of all public Venmo transactions, accessible to anyone via the URL venmo.com/api/v5/public.

189. In addition to this real-time data, Defendant made data about past transactions available via the Venmo API until in or around July 2018.

190. The Venmo transaction data available via the API was even more extensive than that published in the app. For both participants in the transaction, the data included the consumer's first name, last name or first initial of the last name, Venmo user name, and a link to the user's photo. This data also included the message sent with the payment, any comments associated with the transactions, and, if the consumer had connected their Venmo account with Facebook, Facebook IDs.

¹¹ An API is a type of software that allows computers or software applications communicate with each other, acting as an intermediary that processes data transfers between systems. Venmo's API was meant to facilitate the Platform's integration with third-party applications.

191. The transaction data available through Venmo's API could be accessed and downloaded in bulk. Defendant put no significant limits on how, or how much, of this data could be accessed until in or around July 2018.

192. Researchers and privacy advocates repeatedly demonstrated the ability to access and use massive amounts of consumers' data via Venmo's API, downloading and analyzing hundreds of millions of individual transactions from millions of users. Even after Defendant removed the ability to access historical data and limited the rate at which real-time data could be accessed, a computer science student was still able to collect more than seven million Venmo transactions by accessing and downloading more than 57,000 transactions per day.

193. At no point did Defendant disclose to consumers that it made personally identifiable Venmo transaction data freely available to anyone on the Internet in a form that allowed it to be accessed, downloaded, analyzed, and exploited in bulk.

194. Before in or around May 2018, Defendant did not tell consumers that their Venmo transactions could be viewed by anyone on the Internet.

195. In May 2018, Defendant settled an administrative complaint filed by the FTC alleging that its transaction privacy settings were misleading, in violation of the FTC Act. The FTC alleged that Venmo's privacy settings deceptively conveyed that selecting "private" meant that transactions would only be viewable by the participants. In reality, transactions could still be public unless a separate "sharing" setting was also set to "only me." Absent that additional setting, a user's privacy choices could be effectively overridden by the privacy settings of the other transaction participant. Only after its settlement with the FTC did Defendant begin informing

consumers that under Venmo’s default privacy settings, “everyone on the Internet can see, comment [on], and enjoy” their Venmo transactions.¹²

196. Even these enforcement-driven disclosures, however, failed to inform consumers that Defendant continued to publish this information via a freely accessible API that allowed anyone to vacuum up personally identifiable transaction data in bulk. A reasonable consumer would not expect any company—much less a financial institution—to provide such free and materially unlimited access to such sensitive data.

197. There is no apparent business purpose for making all Venmo transactions publicly available through an API without requiring any form of authentication. Privacy and security experts described the practice as “baffling.” Such authentication is a standard requirement for allowing a third-party application or developer to access a company’s data through an API, and Defendant itself requires such authentication when third parties access the PayPal API.

198. Defendant’s use of a public API, allowing free access to personally identifiable Venmo transaction data, prevented consumers from being able to reasonably avoid sharing sensitive financial information without their knowledge, increasing their vulnerability to fraud and harassment, among other harms.

199. This practice is material to consumers. Consumers’ Venmo transaction information is sensitive, detailing when and how frequently a consumer sends and receives money on the app, to whom, and for what purpose. Venmo transaction information can reveal a user’s location, living arrangements, personal and romantic relationships, debt payments, and even illicit activity like selling or purchasing drugs. A study of 389 million Venmo transactions found that 37.8 percent of

¹² Filed simultaneously with its administrative complaint was a Settlement and Proposed Consent Decree in which Defendant agreed to change various disclosures to resolve the administrative complaint. that settlement was ultimately approved by the Commission.

consumers revealed sensitive information about health conditions, political orientation, drug/alcohol consumption, or similarly personal information in their transaction descriptions.

200. Publishing this data exacerbates the risk of fraud, harassment, and other harms discussed in Section V.B, *supra*. Added to personal account and friends information, information about who a person transacts with most often, transacted with most recently, and for what purposes, further exposes consumers to convincing and sophisticated social engineering attacks. Consumers have reported being flooded with payment requests from strangers after engaging in a public Venmo transaction. And location information contained in transaction descriptions can facilitate harassment and stalking in the real world, not just online.

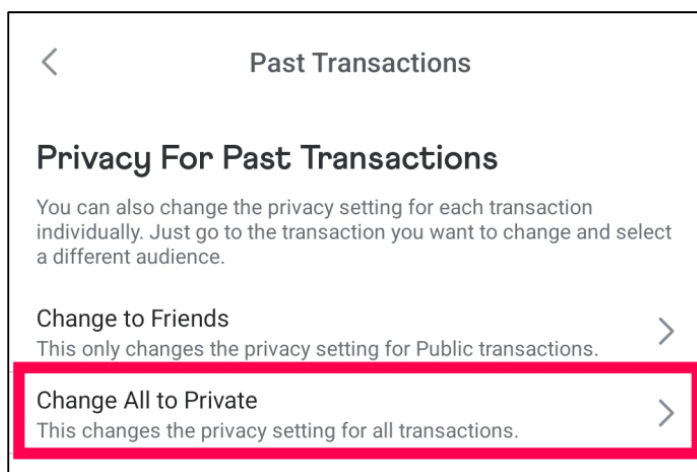
201. Publicizing personally identifiable financial transaction information violates consumer privacy preferences. In a 2018 consumer survey, 77 percent of consumers said mobile payment apps should not be permitted to publish personal transaction information to everyone on the internet.

D. Defendant Misrepresents Venmo Users' Ability to Protect the Privacy of Past Transactions.

202. Consumers are unable to fully assess the extent to which Defendant has made their Venmo transaction information public because Defendant misrepresents users' ability to change the privacy settings on past Venmo transactions.

203. Defendant offers a Venmo privacy setting that purports to allow consumers to change the privacy of past transactions. This setting has existed since at least November 2016.

204. After navigating to the Settings menu, clicking on "Privacy," and selecting "Past Transactions," Defendant provides options that it represents will limit the visibility of past transactions to a user's friends or to "private," which Defendant elsewhere describes as "[v]isible to sender and recipient only."



205. Consumers that select “Change All to Private” are met with a pop-up confirming their privacy selection, which again represents that consumers can make all of their past transactions private.

206. In fact, these privacy settings do not—and cannot—restrict the visibility of formerly public transactions. While these settings allow consumers to alter the visibility of past transactions *on the Venmo platform*, they do nothing to protect the transactions Defendant published in real time via the Venmo API. The transaction data that Defendant purports to allow consumers to retroactively restrict already could have been—and in hundreds of millions of cases, was—accessed, viewed, and downloaded by anyone on the Internet.

207. Defendant thus deceptively conveys to consumers that they can, retroactively, keep private information that Defendant made available to everyone, not just on Venmo, but on the Internet. Defendant cannot un-ring that bell.

208. The ability to adjust the privacy of past transactions is material to consumers—particularly because Defendant makes Venmo transactions public by default. Consumers may choose not to use Venmo’s services if they knew that personally identifiable Venmo transaction information, once published, could not retroactively be made private.

VIOLATIONS OF LAW

COUNT I: Unfair or Deceptive Acts or Practices in Violation of HRS § 480-2(a)

209. Plaintiff repeats and realleges each and every allegation contained in the preceding paragraphs as though set forth fully herein.

210. Defendant has engaged, and continues to engage, in deceptive acts and practices in the conduct of trade or commerce in Hawai‘i, in violation of HRS § 480-2(a). These acts and practices have a tendency to mislead consumers acting reasonably under the circumstances, and are material to consumers. As alleged herein, Defendant has violated HRS § 480-2(a) by:

- a. misrepresenting that consumers can freely access and control the funds in their Venmo and PayPal accounts;
- b. omitting and/or failing to disclose that Defendant suspends, deactivates, and seizes funds from consumers’ Venmo and PayPal accounts, without notice, explanation, or effective recourse;
- c. misrepresenting that Defendant protects consumers’ PayPal and Venmo accounts against losses from fraudulent and unauthorized transactions and assists consumers victimized by fraud;
- d. omitting and/or failing to disclose that Defendant does not limit consumers’ liability for losses of PayPal and Venmo account funds caused by fraud if consumers are fraudulently induced to send the lost funds;
- e. misrepresenting that consumers on the Venmo Platform receive Purchase Protection, and are entitled to a full refund if something goes wrong with a purchase, by indicating that the transaction is a purchase of a good or service;

- f. omitting and/or failing to disclose to consumers on the Venmo Platform that only certain transactions for goods or services are eligible for Purchase Protection;
- g. Misrepresenting that consumers' financial information is "hidden" and "not shared," and that Venmo allows consumers to send payments without sending "account details";
- h. misrepresenting that consumers' personally identifiable Venmo account information and personal contacts will be used for limited purposes;
- i. omitting and/or failing to disclose to consumers on the Venmo Platform that Defendant makes consumers' personally identifiable Venmo account information publicly available by default, and that there is or was no way for consumers to keep this information private;
- j. omitting and/or failing to disclose that Defendant published consumers' personally identifiable Venmo transaction data via a public, freely accessible API; and
- k. misrepresenting that consumers have the ability to limit the visibility past Venmo transactions.

211. Defendant has engaged, and continues to engage, in unfair acts and practices in the conduct of trade or commerce in Hawai'i, in violation of HRS § 480-2(a). These acts and practices cause substantial injury to consumers, offend established public policy, and/or are immoral, ethical, oppressive, or unscrupulous. As alleged herein, Defendant has violated HRS 480-2(a) by:

- a. suspending, deactivating, and seizing funds from consumers' Venmo and PayPal accounts, without notice, explanation, or effective recourse;

- b. charging a Purchase Protection fee on transactions that do not qualify under the terms of the Purchase Protection program and providing no way to contest such improperly assessed fees; and
- c. exposing consumers to fraud, monetary loss, embarrassment, and emotional distress by making public consumers' personally identifiable Venmo account information, including names, Venmo account names, profile pictures, transaction data, and personal contacts.

212. Each and every instance in which Defendants engaged in such unfair or deceptive acts or practices constitutes a separate and independent violation of HRS § 480-2(a).

COUNT II: Deceptive Trade Practices in Violation of HRS § 481A-3(a)

213. Plaintiff repeats and realleges each and every allegation contained in the preceding paragraphs as though set forth fully herein.

214. Defendant has engaged, and continues to engage, in deceptive trade practices in the course of its business, in violation of HRS § 481A-3(a), including by representing that Defendant's goods or services have sponsorship, approval, characteristics, uses, or benefits that they do not have, in violation of HRS § 481A-(3)(a)(5); and by engaging in conduct that creates a likelihood of confusion and misunderstanding, in violation of HRS § 481A-3(a)(12). As alleged herein, Defendant has violated HRS § 481A-3(a) by:

- a. misrepresenting that consumers can freely access and control the funds in their Venmo and PayPal accounts;
- b. omitting and/or failing to disclose that Defendant suspends, deactivates, and seizes funds from consumers' Venmo and PayPal accounts, without notice, explanation, or effective recourse;

- c. misrepresenting that Defendant protects consumers' PayPal and Venmo accounts against losses from fraudulent and unauthorized transactions and assists consumers victimized by fraud;
- d. omitting and/or failing to disclose that Defendant does not limit consumers' liability for losses of PayPal and Venmo account funds caused by fraud if consumers are fraudulently induced to send the lost funds;
- e. misrepresenting that consumers on the Venmo Platform receive Purchase Protection, and are entitled to a full refund if something goes wrong with a purchase, by indicating that the transaction is a purchase of a good or service;
- f. omitting and/or failing to disclose to consumers on the Venmo Platform that only certain transactions for goods or services are eligible for Purchase Protection;
- g. Misrepresenting that consumers' financial information is "hidden" and "not shared," and that Venmo allows consumers to send payments without sending "account details";
- h. misrepresenting that consumers' personally identifiable Venmo account information and personal contacts will be used for limited purposes;
- i. omitting and/or failing to disclose to consumers on the Venmo Platform that Defendant makes consumers' personally identifiable Venmo account information publicly available by default, and that there is or was no way for consumers to keep this information private;

- j. omitting and/or failing to disclose that Defendant published consumers' personally identifiable Venmo transaction data via a public, freely accessible API; and
- k. misrepresenting that consumers have the ability to limit the visibility past Venmo transactions.

215. Each and every instance in which Defendant engaged in these deceptive trade practices constitutes a separate and independent violation of HRS § 481A-3(a).

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays that this court:

A. Find, order, adjudge, and declare that Defendant's conduct as alleged herein violates the statutory provisions set forth herein and other applicable Hawai'i law.

B. Issue an order pursuant to HRS §§ 480-15, 481A-4 and 487-15, permanently enjoining Defendant, its agents, employees, successors, and assigns, directly or indirectly, individually or in concert with others, or through any corporate or other device from engaging in unfair or deceptive acts or practices in violation of HRS § 480-2 and from engaging in deceptive trade practices in violation of HRS 481A-3.

C. Pursuant to HRS § 480-3.1, assess non-compensatory civil fines and penalties in the amount of \$10,000.00 against Defendants for each and every violation of HRS § 480-2 and enter judgment in favor of the Plaintiff accordingly.

D. Pursuant to HRS § 480-15 and § 481A-4, and other applicable Hawai'i law, order the disgorgement of any moneys obtained by Defendant as a result of any of the wrongful acts referenced in this Complaint, or any other acts or omissions in violation of HRS § 480-2(a); award full restitution, including the cost of distributing any restitution fund to affected consumers, as well as pre- and post-judgment interest, against the Defendant, pursuant to HRS § 487-14, including

the court's inherent authority to afford litigants enter full and complete relief and other applicable Hawai'i law, and to enter judgment accordingly.

E. Assess and award judgment in favor of the Plaintiff and against the Defendant for attorneys' fees and costs, cost of the investigation, pre- and post-judgment interest and other reasonable expenses.

F. Assess and award all additional remedies available pursuant to HRS §§ 480 and 481A.

G. Award Plaintiff such other and further relief as the court may deem just and equitable under the circumstances.



Plaintiff affirmatively alleges that it seeks judgment in an amount in excess of the minimum jurisdictional requirements of this Court.

DATED: Honolulu, Hawai'i, December 19, 2022.

/s/ Patrick F. McTernan

L. RICHARD FRIED, JR.
PATRICK F. McTERNAN

Attorneys for Plaintiff

<p align="center">STATE OF HAWAI'I CIRCUIT COURT OF THE FIRST CIRCUIT</p>	<p align="center">SUMMONS TO ANSWER CIVIL COMPLAINT</p>	<p>CASE NUMBER</p>
<p>PLAINTIFF STATE OF HAWAI'I, by its Office of Consumer Protection</p>		<p align="center">VS.</p> <p>DEFENDANT(S) PAYPAL, INC., a Delaware corporation, and PAYPAL HOLDINGS, INC., a Delaware corporation</p>
<p>PLAINTIFF'S NAME & ADDRESS, TEL. NO. L. RICHARD FRIED, JR. 0764-0 PATRICK F. MCTERNAN 4269-0 841 Bishop Street, Suite 600 Honolulu, Hawai'i 96813</p>		
<p>TO THE ABOVE-NAMED DEFENDANT(S)</p> <p>You are hereby summoned and required to file with the court and serve upon</p> <p>L. Richard Fried, Jr. and Patrick F. McTernan 841 Bishop Street, Suite 600, Honolulu, HI 96813</p> <hr/> <p>plaintiff's attorney, whose address is stated above, an answer to the complaint which is herewith served upon you, within 20 days after service of this summons upon you, exclusive of the date of service. If you fail to do so, judgment by default will be taken against you for the relief demanded in the complaint.</p> <p>THIS SUMMONS SHALL NOT BE PERSONALLY DELIVERED BETWEEN 10:00 P.M. AND 6:00 A.M. ON PREMISES NOT OPEN TO THE GENERAL PUBLIC, UNLESS A JUDGE OF THE ABOVE-ENTITLED COURT PERMITS, IN WRITING ON THIS SUMMONS, PERSONAL DELIVERY DURING THOSE HOURS.</p> <p>A FAILURE TO OBEY THIS SUMMONS MAY RESULT IN AN ENTRY OF DEFAULT AND DEFAULT JUDGMENT AGAINST THE DISOBEYING PERSON OR PARTY.</p>		
<p>The original document is filed in the Judiciary's electronic case management system which is accessible via eCourt Kokua at: http://www.courts.state.hi.us</p>	<p align="center">Effective Date of 28-Oct-2019 Signed by: /s/ Patsy Nakamoto Clerk, 1st Circuit, State of Hawai'i</p> 	
 <p>In accordance with the Americans with Disabilities Act, and other applicable state and federal laws, if you require a reasonable accommodation for a disability, please contact the ADA Coordinator at the Circuit Court Administration Office on OAHU- Phone No. 808-539-4400, TTY 808-539-4853, FAX 539-4402, at least ten (10) working days prior to your hearing or appointment date.</p>		