

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW HAMPSHIRE

JAMES HARPER	:	
	:	CIVIL ACTION NO.: 1-20-cv-00771
	:	
Plaintiff,	:	COMPLAINT
	:	
v.	:	JURY TRIAL DEMANDED
	:	
CHARLES P. RETTIG,	:	
IN HIS OFFICIAL CAPACITY AS	:	
COMMISSIONER	:	
INTERNAL REVENUE SERVICE,	:	
	:	
&	:	
	:	
INTERNAL REVENUE SERVICE,	:	
	:	
&	:	
	:	
JOHN DOE IRS AGENTS 1-10,	:	
	:	
	:	
Defendants.	:	

FIRST AMENDED COMPLAINT

The Framers of the Constitution would hardly recognize the unbridled power that the Internal Revenue Service regularly exerts to seize innocent Americans’ private financial information. “The Fourth Amendment refers to ‘papers’ because the Founders understood the seizure of papers to be an outrageous abuse distinct from general warrants.” Donald A. Dripps, *“Dearest Property”: Digital Evidence and the History of Private “Papers” As Special Objects of Search and Seizure*, 103 J. Crim. L. & Criminology 49, 52 (2013). Thus, “[i]f one goes back to the early Republic ... it is difficult to find any federal executive body that could bind subjects to appear, testify, or produce records.” Philip Hamburger, *Is Administrative Law Unlawful?* 221 (2014). Indeed, it was so well established at common law that “[p]apers are the owner’s goods

and chattels” and “are his dearest property” that “it may be confidently asserted that [these] propositions were in the minds of those who framed the fourth amendment to the constitution, and were considered as sufficiently explanatory of what was meant by unreasonable searches and seizures.” *Boyd v. United States*, 116 U.S. 616, 638 (1886) (quoting *Entick v. Carrington*, 19 How. St. Tr. 1029 (1765)). The Supreme Court therefore recognized that “a compulsory production of a man’s private papers” is the same as “[b]reaking into a house and opening boxes and drawers,” and constitutes an unlawful “invasion of his indefeasible right of personal security, personal liberty and private property[.]” *Id.* at 622, 630.

Yet, given changes in technology, business and social practices, the law has drifted from these cherished principles and the fundamental understanding that informed the Constitution’s protections. Where once it lacked the authority to peek into a person’s private papers even *with* the use of a subpoena, the Internal Revenue Service has now acquired the power to demand access to anyone’s private information *without any* judicial process. IRS demands access even when a person has entered into a contract with a third party that promises to protect his private information from such intrusion.

This case presents the opportunity to correct the course of constitutional law. Where a person, like Mr. Harper, contracts with a third party to hold his private financial information private including against government intrusion, he does not “voluntarily assume the risk of [the party] turning over” the data. *Carpenter v. United States*, 138 S. Ct. 2206, 2219 (2018). Indeed, he expects the opposite—that the third party *and the government* will respect his contractual rights. Defendants have unlawfully violated those expectations, in defiance of the Fourth and Fifth Amendments and statutory protections.

PARTIES

1. Plaintiff James Harper is a natural person and a resident of the State of New Hampshire.
2. On August 9, 2019, Mr. Harper received a letter from Defendant Internal Revenue Service (IRS) informing him that his financial records related to ownership of bitcoin had been obtained by Defendant IRS without any particularized suspicion of wrongdoing.
3. Defendant Charles R. Rettig is the agency head of IRS and is sued in his official capacity as Commissioner of IRS.
4. Defendant IRS is an agency of the United States, which obtained Mr. Harper's private financial information.
5. Defendant John Doe IRS Agents 1 through 10 are fictitious names for the person(s) who authorized and conducted the unlawful search of Mr. Harper's private financial records.
6. Defendants Doe are sued in their personal capacities.

JURISDICTION AND VENUE

7. This Court has federal question jurisdiction pursuant to 28 U.S.C. § 1331.
8. This Court has the authority to grant declaratory and injunctive relief in this matter pursuant to 28 U.S.C. §§ 2201 and 2202.
9. Venue for this action properly lies in this district pursuant to 28 U.S.C. §§ 1391(b)(2), (e)(1)(C) because Mr. Harper resides in this judicial district, a substantial part of the events or omissions giving rise to the claim occurred in this judicial district, and because the property at issue in this action is situated in this judicial district.

STATEMENT OF FACTS

I. IRS'S STATUTORY SUBPOENA POWER

10. 26 U.S.C. § 7602(a), purports to give IRS the statutory authority to issue administrative summonses.

11. That code section says that IRS may issue summonses for the purposes of “ascertaining the correctness of any return, making a return where none has been made, determining the liability of any person for any internal revenue tax or ... collecting any such liability.” 26 U.S.C. § 7602(a).

12. Where IRS issues a summons to a third-party recordkeeper to gather information about a taxpayer, IRS must notify the taxpayer of the summons pursuant to 26 U.S.C. § 7609(a).

13. Taxpayers may petition to quash such summonses, and IRS may petition to enforce them. 26 U.S.C. §§ 7604, 7609.

14. “Regardless of who initiates the action, the court follows a familiar structured analysis in a summons enforcement proceeding.” *Sugarloaf Funding, LLC v. U.S. Dep’t of the Treasury*, 584 F.3d 340, 345 (1st Cir. 2009). “The IRS must first make a prima facie showing [1] that the investigation will be conducted pursuant to a legitimate purpose, [2] that the inquiry may be relevant to the purpose, [3] that the information sought is not already within the Commissioner’s possession, and [4] that the administrative steps required by the Code have been followed.” *Id.* (citation omitted). Once the IRS has made this showing, the burden shifts to the taxpayer to disprove one or more of the requirements, or to show that enforcement would be “an abuse of process, e.g., that the summons was issued in bad faith for an improper purpose.” *Id.* at 346 (citation omitted).

15. Sometimes, however, the IRS seeks information “where the IRS *does not know* the identity of the taxpayer under investigation[.]” *Tiffany Fine Arts, Inc. v. United States*, 469 U.S. 310, 317 (1985). In such cases, the IRS must comply with 26 U.S.C. § 7609(f). *Id.*

16. “Congress passed section 7609(f) specifically to protect the civil rights, including the privacy rights, of taxpayers subjected to the IRS’s aggressive use of third-party summonses.” *United States v. Gertner*, 65 F.3d 963, 971 (1st Cir. 1995). “Section 7609(f) accomplishes this goal by providing that a John Doe summons is not valid unless and until it is authorized by a judicial officer after a hearing” where the IRS must establish that:

(1) the summons relates to the investigation of a particular person or ascertainable group or class of persons,

(2) there is a reasonable basis for believing that such person or group or class of persons may fail or may have failed to comply with any provision of any internal revenue law, and

(3) the information sought to be obtained from the examination of the records (and the identity of the person or persons with respect to whose liability the summons is issued) is not readily available from other sources.

Id. at 971-72 (citing 26 U.S.C. § 7609(f)).

17. “This requirement of judicial preapproval is an important component of the statutory scheme; it permits the district court to act as a surrogate for the unnamed taxpayer and to ‘exert a restraining influence on the IRS.’” *Id.* (quoting *Tiffany Fine Arts, Inc.*, 469 U.S. at 321). “The statutory protections cannot be cavalierly cast aside by either the executive or the judicial branch.” *Id.*

II. MR. HARPER’S USE OF BITCOIN

18. In 2013 Mr. Harper opened an account with Coinbase, a non-party digital currency exchange that facilitates transactions in virtual currencies such as bitcoin.

19. Through the opening of his account, Mr. Harper and Coinbase contracted according to Coinbase's Terms of Service. (Exhibit 1.)

20. Section 9.4 of the agreement "incorporated by reference" Coinbase's "Privacy Policy." (Exhibits 1, 2 (privacy policy).)

21. Coinbase's 2013 Privacy Policy applied to "personal information," which Coinbase defined as "information that can be associated with a specific person [that] can be used to identify that person." (Exhibit 1.)

22. Coinbase said it would "store and process [Mr. Harper's] personal and transactional information, including certain payment information, such as [his] encrypted bank account and/or routing numbers, on our computers in the United States and elsewhere in the world where Coinbase facilities or our service providers are located[.]" (Exhibit 2.)

23. Coinbase also provided, "We store our customers' personal information securely throughout the life of the customer's Coinbase Account. Coinbase will retain your personal information for a minimum of five years or as necessary to comply with our legal obligations or resolve disputes." (Exhibit 2.)

24. Coinbase also contracted to protect this personal information. (Exhibit 2.)

25. The agreement said, "Coinbase takes reasonable precautions, as described herein, to protect your personal information from loss, misuse, unauthorized access, disclosure, alteration, and destruction." (Exhibit 2.)

26. Coinbase said it would "protect" personal information "by maintaining physical, electronic and procedural safeguards in compliance with applicable US federal and state regulations" and by using "computer safeguards such as firewalls and data encryption," "physical access controls to our buildings and files," including "authoriz[ing] access to personal

information only for those employees who require it to fulfill their job responsibilities” and storing “[f]ull credit card data” “hosted off-site by a payment vendor in compliance with Payment Card Industry Data Security Standards (PCI DSS).” (Exhibit 2.)

27. Coinbase said:

Our primary purpose in collecting personal information is to provide you with a secure, smooth, efficient, and customized experience. We may use your personal information to:

Provide Coinbase Services and customer support you request;

Process transactions and send notices about your transactions;

Resolve disputes, collect fees, and troubleshoot problems;

Prevent and investigate potentially prohibited or illegal activities, and/or violations of our posted user terms;

Customize, measure, and improve Coinbase Services and the content and layout of our website and applications;

Deliver targeted marketing, service update notices, and promotional offers based on your communication preferences; and

Compare information for accuracy and verify it with third parties.

We will not use your personal information for purposes other than those purposes we have disclosed to you, without your permission.

(Exhibit 2.)

28. Coinbase said:

We may share your personal information with:

Service providers under contract who help with parts of our business operations such as fraud prevention, bill collection, marketing and technology services. Our contracts dictate that these service providers only use your information in connection with the services they perform for us and not for their own benefit.

Financial institutions with which we partner.

Companies that we plan to merge with or be acquired by. (Should such a combination occur, we will require that the new combined entity follow this Privacy Policy with respect to your personal information. You will receive prior notice of any change in applicable policy.)

Law enforcement, government officials, or other third parties when:

We are compelled to do so by a subpoena, court order or similar legal procedure; or

We believe in good faith that the disclosure of personal information is necessary to prevent physical harm or financial loss, to report suspected illegal activity or to investigate violations of our User Agreement.

Other third parties with your consent or direction to do so.

(Exhibit 2.)

29. During 2013 and 2014 Mr. Harper made a series of deposits of bitcoin in his Coinbase account—primarily as income from consulting work.

30. Mr. Harper declared these transactions on a 2013 tax return for a consulting entity and declared all appropriate income from bitcoin payments.

31. Mr. Harper also reported and paid capital gains tax on his bitcoin income for that tax year.

32. Mr. Harper continued to receive consulting income in bitcoin in 2014, which he deposited in his Coinbase account through monthly purchases of approximately \$3,500.

33. Mr. Harper's consultancy also reported this income on his 2014 tax return and reported a capital loss for his bitcoin holdings for that tax year.

34. In 2015 Mr. Harper stopped accumulating new bitcoin and began liquidating his investments via Coinbase.

35. During the fall of 2015 Mr. Harper began transferring his remaining holdings in Coinbase to a hardware wallet.

36. By early 2016 Mr. Harper no longer held bitcoin on Coinbase's platform.

37. Mr. Harper reported and paid appropriate capital gains on any bitcoin income for tax years 2015 and 2016.

38. In 2016 IRS filed an *ex parte* "John Doe" administrative summons on Coinbase in the U.S. District Court for the Northern District of California pursuant to 26 U.S.C. § 7609(h). *See United States v. Coinbase, Inc.*, No. 17-cv-1431, 2017 WL 5890052, at *1 (N.D. Cal. 2017) (Scott Corley, U.S.M.J.).

39. The Initial Summons sought "information regarding United States persons who at any time during the period January 1, 2013 through December 31, 2015 conducted transactions in a convertible virtual currency as defined in IRS Notice 2014-21." *Id.*

40. The summons requested nine categories of documents including: complete user profiles, know-your-customer due diligence, documents regarding third-party access, transaction logs, records of payments processed, correspondence between Coinbase and Coinbase users, account or invoice statements, records of payments, and exception records produced by Coinbase's AML system. *Id.*

41. Coinbase opposed the summons, and IRS narrowed it slightly. *Id.* at *2.

42. As modified, IRS sought information regarding accounts "with at least the equivalent of \$20,000 in any one transaction type (buy, sell, send, or receive) in any one year during the 2013-2015 period." *Id.*

43. The Narrowed Summons "d[id] not include users: (a) who only bought and held bitcoin during the 2013-15 period; or (b) for which Coinbase filed Forms 1099-K during the 2013-15 period." *Id.*

44. According to Coinbase, the Narrowed Summons requested information regarding 8.9 million transactions and 14,355 account holders. *Id.* at *4.

45. For those accounts, IRS sought the following records:

- Request 1: Account/wallet/vault registration records for each account/wallet/vault owned or controlled by the user during the period stated above limited to name, address, tax identification number, date of birth, account opening records, copies of passport or driver's license, all wallet addresses, and all public keys for all accounts/wallets/vaults.
- Request 2: Records of Know-Your-Customer diligence.
- Request 3: Agreements or instructions granting a third-party access, control, or transaction approval authority.
- Request 4: All records of account/wallet/vault activity including transaction logs or other records identifying the date, amount, and type of transaction (purchase/sale/exchange), the post transaction balance, the names or other identifiers of counterparties to the transaction; requests or instructions to send or receive bitcoin; and, where counterparties transact through their own Coinbase accounts/wallets/vaults, all available information identifying the users of such accounts and their contact information.
- Request 5: Correspondence between Coinbase and the user or any third party with access to the account/wallet/vault pertaining to the account/wallet/vault opening, closing, or transaction activity.
- Request 6: All periodic statements of account or invoices (or the equivalent).

Id. at 2.

46. Coinbase refused to comply with the summons, and IRS petitioned to enforce the summons against Coinbase pursuant to 26 U.S.C. § 7402(b) and 7604(a). *Id.* at *1.

47. After the Narrowed Summons was issued, at least one target of the summons learned of its existence and sought permission to intervene as a John Doe. *See Coinbase, Inc.*, 3:17-cv-1431, Doc. 40, at 4-5 (July 18, 2017).

48. The reviewing United States Magistrate Judge granted the John Doe leave to intervene, but only to the extent the John Doe presented argument that the summons violated the standard applicable to direct summonses under 26 U.S.C. § 7602. *Id.* at 7.

49. The Magistrate Judge noted that it had already determined IRS met the standard applicable to John Doe summonses set out in 26 U.S.C. § 7609(f) in an *ex parte* hearing and did not revisit that decision. *See id.* at 5.

50. Mr. Harper was not provided notice of the summons or provided an opportunity to directly intervene in the petition to enforce.

51. Mr. Harper did, however, participate as an expert in an amicus filing accepted by the Magistrate Judge in its consideration of the petition to enforce.

52. After a hearing, the Magistrate Judge upheld Requests 1, 4 and 6 based on the standard announced in *United States v. Powell*, 379 U.S. 48 (1964). *Coinbase, Inc.*, 2017 WL 5890052 at * 8-9.

53. The Magistrate Judge did not apply the heightened John Doe summons standard set out in 26 U.S.C. § 7609(f). *See id.*

54. Specifically, the Magistrate Judge ordered Coinbase “to produce” “for accounts with at least the equivalent of \$20,000 in any one transaction type (buy, sell, send, or receive) in any one year during the 2013 to 2015 period:

- (1) the taxpayer ID number,
- (2) name,
- (3) birth date,
- (3) address,

(4) records of account activity including transaction logs or other records identifying the date, amount, and type of transaction (purchase/sale/exchange), the post transaction balance, and the names of counterparties to the transaction, and

(5) all periodic statements of account or invoices (or the equivalent).

Id.

55. Neither party appealed to a higher court.

56. From 2016 to present, Mr. Harper and his wife liquidated bitcoin through either Abra or Uphold digital exchanges.

57. Abra and Uphold, which are nonparties to this action, both contractually incorporated privacy policies into their terms of service. (Exhibits 3 (Abra Terms of Service), 4 (Uphold Terms of Service).)

58. Abra defined “personal information” as “any information relating to an identified or identifiable natural person (each, a ‘Data Subject’); an identifiable natural person is one who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, or an online identifier or to one or more factors specific to the physical, economic, cultural or social identity of that natural person.” (Exhibit 3.)

59. Abra’s policy said,

We take the protection and storage of your personal data very seriously and take all reasonable steps to ensure the ongoing confidentiality, integrity, and availability of your personal data. We protect your personal data by using reasonable security safeguards against loss or theft, unauthorized access, disclosure, copying, use, or modification. Your personal data is stored behind secured networks and is accessible by a limited number of persons who have special access rights to such systems and are required to keep the personal data confidential. We implement a variety of security measures, such as encryption and anonymization when users enter, submit, or access their personal data to maintain the safety of their personal data.

(Exhibit 3.)

60. Abra provided that it “may, under certain circumstances and in its sole discretion, disclose your information if we believe that it is reasonable to do so. Such disclosure or transfer is limited to situations where the personal data are required for the purposes of (1) provision of the services, (2) pursuing our legitimate interests, (3) law enforcement purposes, or (4) if you provide your prior explicit consent.” (Exhibit 3.)

61. Abra said that such reasonable disclosure cases may include:

- Satisfying any local, state, or Federal laws or regulations;
- Responding to requests, such as discovery, criminal, civil, or administrative process, subpoenas, court orders, or writs from law enforcement or other governmental or legal bodies;
- Bringing legal action against a user who has violated the law or violated our Terms of Use;
- As may be necessary for the operation of Abra;
- Generally cooperating with any lawful investigation about our users; or
- If we suspect any fraudulent activity or have noticed any activity which may violate our Terms of Use or other applicable rules.

(Exhibit 3.)

62. Uphold agreed that it “may also release your information to certified and authorized law enforcement officials when we believe release is appropriate to comply with the law, enforce our terms or policies, or protect the rights, property, or safety of Uphold, our members, or others.” (Exhibit 4.)

63. In a separate provision, Uphold set out the circumstances where it would comply with “United States Law Enforcement” requests for information:

We disclose records in accordance with our Membership Agreement and applicable law, including the federal Stored Communications Act (“SCA”), 18 U.S.C. § 2701 *et seq.*

A. We require a valid subpoena issued in connection with an official criminal investigation for the disclosure of basic subscriber records (defined in 18 U.S.C. § 2703(c)(2)), which may include: name, length of service, credit card information, email address(es), and recent IP address(es), if available.

B. We require a court order issued under 18 U.S.C. § 2703(d) for the disclosure of certain records or other information pertaining to the account, not including any contents of communications, which may include message headers and IP addresses, in addition to the basic subscriber records identified above.

C. We require a search warrant issued under the procedures described in the Federal Rules of Criminal Procedure or equivalent state warrant procedures upon a showing of probable cause for the disclosure of any stored content, which may include available messages sent with a transfer, if any.

D. We interpret the national security letter provision as applied to us to require the production of only: name and length of service.

(Exhibit 5.)

64. Mr. Harper declared capital gains for his bitcoin holdings for tax years 2016, 2017, 2018 and 2019.

65. Mr. Harper has paid all applicable taxes for those gains.

66. Mr. Harper will continue to declare and pay capital gains and other applicable taxes for his bitcoin holdings, if any, for tax year 2020, and for each tax year in the future.

67. On August 9, 2019, Mr. Harper received a letter titled “Reporting Virtual Currency Transactions” from IRS. (Exhibit 6.)

68. The letter said, “We have information that you have or had one or more accounts containing virtual currency but may not have properly reported your transactions involving virtual currency, which include cryptocurrency and non-crypto virtual currencies.” (Exhibit 6.)

69. The letter warned that if Mr. Harper had not “accurately report[ed his] virtual currency transactions” he “may be subject to future civil and criminal enforcement activity.” (Exhibit 6.)

70. Mr. Harper has no significant financial records related to accounts containing bitcoin or other virtual currency transactions other than those related to his accounts with Abra, Coinbase or Uphold.

71. On July 20, 2020, *i.e.*, after the Complaint was filed, Mark G. Anderson, Secretary and Head of Legal and Regulatory Affairs for Uphold executed a notarized affidavit in support of the Plaintiff. (Exhibit 8.)

72. Mr. Anderson, in his duly sworn affidavit, speaks for Uphold in an official capacity. (Exhibit 8.) Mr. Anderson is not a party to this lawsuit.

73. Mr. Anderson confirms that Uphold “has conducted a thorough search of its records and has found no record of any request by the Defendants in the above-named action to produce information relating to the Plaintiff.” (Exhibit 8.)

74. Uphold confirms that it “has conducted a thorough search of its records and has found no record of any information relating to the Plaintiff having been directly disclosed to the Defendants.” (Exhibit 8.)

75. Mr. Harper has accurately reported his virtual currency transactions for all applicable tax years.

76. Upon information and belief, John Doe IRS Agents 1 through 10 issued an informal demand for Mr. Harper’s financial records to Abra, and/or Coinbase, with which one or more of the exchanges complied.

77. John Doe IRS Agents 1 through 10 and IRS lacked any particularized suspicion that Mr. Harper had violated any law prior to obtaining Mr. Harper's financial records referenced in its August 9, 2019 letter.

78. John Doe IRS Agents 1 through 10 and IRS did not obtain a judicial warrant prior to obtaining Mr. Harper's financial records referenced in its August 9, 2019 letter.

79. John Doe IRS Agents 1 through 10 and IRS did not obtain a subpoena prior to obtaining Mr. Harper's financial records referenced in its August 9, 2019 letter.

80. On information and belief, Abra and/or Coinbase may have violated their respective terms of service in providing Mr. Harper's financial records referenced in IRS's August 9, 2019 letter by disclosing Mr. Harper's records without a valid subpoena, court order, or judicial warrant based on probable cause.

81. Mr. Harper never received any notice of a third-party summons from IRS pursuant to 26 U.S.C. § 7609(a).

82. IRS issued "more than 10,000" similar letters to taxpayers concerning their virtual currency transactions. Press Release, *IRS has begun sending letters to virtual currency owners advising them to pay back taxes, file amended returns; part of agency's larger efforts*, IR-2019-132 (July 26, 2019), available at <https://www.irs.gov/newsroom/irs-has-begun-sending-letters-to-virtual-currency-owners-advising-them-to-pay-back-taxes-file-amended-returns-part-of-agencys-larger-efforts>. (Exhibit 7.)

83. As with Mr. Harper, upon information and belief, IRS obtained private financial records for the targeted taxpayers without first obtaining a judicial warrant or a lawful subpoena or other court order.

84. IRS continues to hold Mr. Harper’s private financial records that it obtained from Abra, Coinbase and/or some other entity or person.

COUNT I: VIOLATION OF THE FOURTH AMENDMENT OF THE U.S. CONSTITUTION (BIVENS AND DECLARATORY ACTION)—THE DEFENDANTS CONDUCTED AN UNLAWFUL SEARCH AND SEIZURE OF MR. HARPER’S PRIVATE FINANCIAL INFORMATION (ALL DEFENDANTS)

85. Plaintiff incorporates by reference all of the preceding material as though fully set forth under Count I.

86. The Fourth Amendment to the U.S. Constitution protects “the right of the people to be secure in their ... papers ... against unreasonable searches and seizures.”

87. “Papers are the owner’s goods and chattels; they are his dearest property, and are so far from enduring a seizure, that they will hardly bear an inspection; and though the eye cannot by the laws of England be guilty of a trespass, yet where private papers are removed and ferried away the secret nature of those goods will be an aggravation of the trespass, and demand more considerable damages in that respect.” *Boyd v. United States*, 116 U.S. 616, 638 (1886) (quoting *Entick v. Carrington*, 19 How. St. Tr. 1029 (1765)).

88. A “compulsory production of a man’s private papers” is no different than “[b]reaking into a house and opening boxes and drawers.” *Id.* at 622, 630. Both involve “the invasion of his indefeasible right of personal security, personal liberty, and private property[.]” *Id.* at 630.

89. Mr. Harper retained a property right in his information pursuant to his contractual agreements with Abra, Coinbase and Uphold.

90. Mr. Harper retained ownership of the personal information he provided to Abra, Coinbase and Uphold and permitted those exchanges to use his information only according to the terms of service agreements.

91. Mr. Harper had a reasonable expectation of privacy in the financial records held by Abra, Coinbase and Uphold related to his accounts containing bitcoin or other virtual currency transactions.

92. Mr. Harper had a subjective expectation of privacy in the financial records held by Abra, Coinbase and Uphold related to his accounts containing bitcoin or other virtual currency transactions.

93. Mr. Harper reasonably expected that Abra, Coinbase and Uphold would abide by the contractual provisions set out in their respective terms of service.

94. Specifically, Mr. Harper reasonably and subjectively expected that Abra would abide by its terms of service, including its agreement that it took “the protection and storage of [Mr. Harper’s] personal data very seriously,” and thus would limit its disclosures to law enforcement to “administrative process, subpoenas, court orders, or writs from law enforcement or other governmental or legal bodies[.]”

95. Mr. Harper also reasonably and subjectively expected that Coinbase would abide by its terms of service, including its agreement to “protect [his] personal information from loss, misuse, unauthorized access, disclosure, alteration, and destruction,” and its promise to only turn the information over to “law enforcement [or] government officials” when it was “compelled to do so by a subpoena, court order or similar legal procedure[.]”

96. Mr. Harper also reasonably and subjectively expected that Uphold would abide by its terms of service, including its agreement that it would only disclose his private information to

law enforcement pursuant to “a valid subpoena issued in connection with an official criminal investigation for the disclosure of basic subscriber records,” “a court order issued under 18 U.S.C. § 2703(d),” or “a search warrant” issued upon “probable cause.”

97. Upon information and belief IRS obtained Mr. Harper’s financial records referenced in its August 9, 2019 letter from Abra, Coinbase and/or some other entity or person.

98. Mr. Harper has no significant financial records related to accounts containing bitcoin or other virtual currency transactions other than those related to his accounts with Abra, Coinbase or Uphold.

99. Mr. Harper has accurately reported his virtual currency transactions for all applicable tax years.

100. Upon information and belief, John Doe IRS Agents 1 through 10 issued an informal demand for Mr. Harper’s financial records to Abra and/or Coinbase, with which one or more of the exchanges complied.

101. John Doe IRS Agents 1 through 10 and IRS lacked any particularized suspicion that Mr. Harper had violated any law prior to obtaining Mr. Harper’s financial records referenced in IRS’s August 9, 2019 letter.

102. John Doe IRS Agents 1 through 10 and IRS did not obtain a judicial warrant prior to obtaining Mr. Harper’s financial records referenced in IRS’s August 9, 2019 letter.

103. John Doe IRS Agents 1 through 10 and IRS did not obtain a subpoena prior to obtaining Mr. Harper’s financial records referenced in IRS’s August 9, 2019 letter.

104. Abra and/or Coinbase violated their respective terms of service in providing Mr. Harper’s financial records referenced in IRS’s August 9, 2019 letter by disclosing Mr. Harper’s records without a valid subpoena, court order or judicial warrant based on probable cause.

105. Mr. Harper never received any notice of a third-party summons from IRS pursuant to 26 U.S.C. § 7609(a).

106. John Doe IRS Agents 1 through 10 and IRS violated the Fourth Amendment by seizing Mr. Harper's private financial information from Abra and/or Coinbase without first acquiring a warrant based on probable cause.

107. To the extent that 26 U.S.C. § 7602(a), *et seq.*, allowed John Doe IRS Agent(s) and IRS to seize Mr. Harper's private financial information without first acquiring a warrant based on probable cause, the statute is unconstitutional as applied to Mr. Harper under the Fourth Amendment.

108. IRS continues to hold Mr. Harper's private financial records that it obtained from Abra, Coinbase, and/or some other entity or person.

109. Unless ordered to expunge Mr. Harper's private financial records, IRS will continue to hold that information unlawfully.

110. Upon information and belief John Doe IRS Agents 1 through 10 and IRS have conducted similar unlawful seizures related to more than 10,000 taxpayers who were sent notices similar to Mr. Harper's.

111. Unless enjoined, John Doe IRS Agents 1 through 10 and IRS will continue to conduct unlawful seizures of private financial information related to virtual currencies held by virtual currency exchanges, including those relying on the purported authority set out by 26 U.S.C. § 7602(a), *et seq.*

112. John Doe IRS Agents 1 through 10 are personally liable for damages for their Fourth Amendment violations. *See Bivens v. Six Unknown Named Agents of Fed. Bureau of Narcotics*, 403 U.S. 388, 389 (1971).

WHEREFORE, Plaintiff, Mr. Harper demands judgment for compensatory damages against Defendants for such sums as would reasonably and properly compensate him for injuries together with delay damages, interest, costs, and attorneys' fees and declaratory and injunctive relief, including an order expunging Mr. Harper's private financial information from IRS's records.

COUNT II: VIOLATION OF THE FIFTH AMENDMENT OF THE U.S. CONSTITUTION (*BIVENS* AND DECLARATORY ACTION)—THE DEFENDANTS VIOLATED DUE PROCESS PROTECTIONS IN SEIZING MR. HARPER'S PRIVATE FINANCIAL INFORMATION (ALL DEFENDANTS)

113. Plaintiff incorporates by reference all of the preceding material as though fully set forth under Count II.

114. The Fifth Amendment to the United States Constitution provides that “[n]o person shall” “be deprived of life, liberty, or property, without due process of law.”

115. Mr. Harper retained a property right in his personal information pursuant to his contractual agreements with Abra, Coinbase and Uphold.

116. Mr. Harper retained ownership of the personal information he provided to Abra, Coinbase and Uphold and permitted those exchanges to use his information only according to the terms of service agreements.

117. Pursuant to those contracts Mr. Harper expected Abra, Coinbase and Uphold to abide by the contractual provisions set out in their respective terms of service.

118. Specifically, Mr. Harper expected that Abra would abide by its terms of service, including its agreement that it took “the protection and storage of [Mr. Harper's] personal data very seriously,” and thus would limit its disclosures to law enforcement to “administrative

process, subpoenas, court orders, or writs from law enforcement or other governmental or legal bodies[.]”

119. Mr. Harper also expected that Coinbase would abide by its terms of service, including its agreement to “protect [his] personal information from loss, misuse, unauthorized access, disclosure, alteration, and destruction,” and its promise to only turn the information over to “law enforcement [or] government officials” when it was “compelled to do so by a subpoena, court order or similar legal procedure[.]”

120. Mr. Harper also expected that Uphold would abide by its terms of service, including its agreement that it would only disclose his private information to law enforcement pursuant to “a valid subpoena issued in connection with an official criminal investigation for the disclosure of basic subscriber records,” “a court order issued under 18 U.S.C. § 2703(d),” or “a search warrant” issued upon “probable cause.”

121. Upon information and belief IRS obtained Mr. Harper’s financial records referenced in its August 9, 2019 letter from Abra, Coinbase, and/or some other entity or person.

122. Mr. Harper has no significant financial records related to accounts containing bitcoin or other virtual currency transactions other than those related to his accounts with Abra, Coinbase or Uphold.

123. Mr. Harper has accurately reported his virtual currency transactions for all applicable tax years.

124. Upon information and belief, John Doe IRS Agents 1 through 10 issued an informal demand for Mr. Harper’s financial records to Abra and/or Coinbase with which one or more of the exchanges complied.

125. John Doe IRS Agents 1 through 10 and IRS did not obtain a judicial warrant prior to obtaining Mr. Harper's financial records referenced in IRS's August 9, 2019 letter.

126. John Doe IRS Agents 1 through 10 and IRS did not obtain a subpoena prior to obtaining Mr. Harper's financial records referenced in IRS's August 9, 2019 letter.

127. Mr. Harper never received any notice of a third-party summons from IRS pursuant to 26 U.S.C. § 7609(a).

128. Abra and/or Coinbase may have violated their respective terms of service in providing Mr. Harper's financial records referenced in IRS's August 9, 2019 letter by disclosing Mr. Harper's records without a valid subpoena, court order or judicial warrant based on probable cause.

129. John Doe IRS Agents 1 through 10 and IRS violated the Due Process Clause of the Fifth Amendment by seizing Mr. Harper's intangible property rights in his private financial information from Abra and/or Coinbase without first providing him notice and an opportunity to challenge the seizure of his property.

130. To the extent that 26 U.S.C. § 7602(a), *et seq.*, allowed John Doe IRS Agents 1 through 10 and IRS to seize Mr. Harper's intangible property rights in his private financial information without first providing direct notice and an opportunity to challenge the seizure of his property, the statute is unconstitutional as applied to Mr. Harper under the Fifth Amendment's Due Process Clause.

131. IRS continues to hold Mr. Harper's private financial records that it obtained from Abra Coinbase, and/or some other entity or person.

132. Unless ordered to expunge Mr. Harper's private financial records, IRS will continue to hold that information unlawfully.

133. Upon information and belief John Doe IRS Agents 1 through 10 and IRS have conducted similar unlawful seizures of intangible property rights in private financial information related to more than 10,000 taxpayers who were sent notices similar to Mr. Harper's.

134. Unless enjoined, John Doe IRS Agents 1 through 10 and IRS will continue to conduct unlawful seizures of intangible property rights in private financial information related to virtual currencies held by virtual currency exchanges, including those relying on the purported authority set out by 26 U.S.C. § 7602(a), *et seq.*

135. John Doe IRS Agents 1 through 10 are personally liable for damages for their Fifth Amendment violation. *See Bivens v. Six Unknown Named Agents of Fed. Bureau of Narcotics*, 403 U.S. 388, 389 (1971).

WHEREFORE, Plaintiff, Mr. Harper demands judgment for compensatory damages against Defendants for such sums as would reasonably and properly compensate him for injuries together with delay damages, interest, costs, and attorneys' fees and declaratory and injunctive relief, including an order expunging Mr. Harper's private financial information from IRS's records.

COUNT III: VIOLATION OF 15 U.S.C. § 7609(f) (DECLARATORY ACTION)—THE DEFENDANTS OBTAINED MR. HARPER'S FINANCIAL RECORDS THROUGH AN UNLAWFUL JOHN DOE SUBPOENA (ALL DEFENDANTS)

136. Plaintiff incorporates by reference all of the preceding material as though fully set forth under Count III.

137. 26 U.S.C. § 7609(f) authorizes IRS to issue John Doe summonses for financial records only if the Secretary establishes that "(1) the summons relates to the investigation of a particular person or ascertainable group or class of persons, (2) there is a reasonable basis for believing that such person or group or class of persons may fail or may have failed to comply

with any provision of any internal revenue law, and (3) the information sought to be obtained from the examination of the records (and the identity of the person or persons with respect to whose liability the summons is issued) is not readily available from other sources.” *United States v. Gertner*, 65 F.3d 963, 971-72 (1st Cir. 1995).

138. Upon information and belief IRS obtained Mr. Harper’s financial records referenced in its August 9, 2019 letter from Abra, Coinbase, and/or some other person or entity.

139. Mr. Harper has no significant financial records related to accounts containing bitcoin or other virtual currency transactions other than those related to his accounts with Abra, Coinbase or Uphold.

140. Mr. Harper has accurately reported his virtual currency transactions for all applicable tax years.

141. Upon information and belief, John Doe IRS Agents 1 through 10 issued a John Doe subpoena under 26 U.S.C. § 7602(a) *et seq.* to Abra and/or Coinbase, with which one or more of the exchanges complied.

142. Mr. Harper never received any notice of a third-party summons from IRS pursuant to 26 U.S.C. § 7609(a).

143. The John Doe summons issued to Abra and/or Coinbase did not relate to a particular person or ascertainable group or class of persons as required by statute, but to all owners of virtual currencies based only on a gross judgment (or guess) that some virtual currency holders may not comply or may not have complied with their tax obligations.

144. John Doe IRS Agents 1 through 10 and IRS lacked a reasonable basis for believing that Mr. Harper failed to comply with any provision of any internal revenue law and

instead John Doe IRS Agents 1 through 10 and IRS issued a John Doe summons that encompassed all innocent owners of virtual currencies.

145. Upon information and belief John Doe IRS Agents 1 through 10 and IRS have conducted similar unlawful seizures of private financial information related to more than 10,000 taxpayers who were sent notices similar to Mr. Harper's following similarly unlawful John Doe summonses.

146. IRS continues to hold Mr. Harper's private financial records that it obtained from Abra, Coinbase, and/or some other entity or person.

147. Unless ordered to expunge Mr. Harper's private financial records, IRS will continue to hold that information unlawfully.

148. Unless enjoined, John Doe IRS Agents 1 through 10 and IRS will continue to conduct unlawful seizures of private financial information related to virtual currencies held by virtual currency exchanges in violation of the limits set out in 26 U.S.C. § 7609(f).

WHEREFORE, Plaintiff, Mr. Harper demands a declaratory judgment and injunctive relief against Defendants, including an order expunging Mr. Harper's private financial information from IRS's records.

JURY DEMAND

Plaintiff demands a trial by jury of all triable issues in the present matter.

August 5, 2020

Respectfully submitted.

Jared Bedrick
Douglas, Leonard & Garvey, P.C.
14 South Street
Concord, NH 03301
N.H. Bar No. 20438
(603)224-1988

jbedrick@nhlawoffice.com

Caleb Kruckenberg*

Litigation Counsel

Aditya Dynar*

Litigation Counsel

New Civil Liberties Alliance

1225 19th St. NW, Suite 450

Washington, DC 20036

(202) 869-5230

caleb.kruckenberg@ncla.legal

adi.dynar@ncla.legal

*Applications for Admission *Pro*

Hac Vice to be filed

coinbase



Please sign in first to perform this action.

[Privacy Policy](#)[User Agreement](#)

Effective Date: August 1st, 2012. Last updated: June 11th, 2013.

This User Agreement ("Agreement") is a contract between you and Coinbase and applies to your use of Coinbase services. You must read, agree with and accept all of the terms and conditions contained in this Agreement.

This is an important document which you must consider carefully when choosing whether to use Coinbase services.

Please note the following risks of using Coinbase services:

- Bitcoin purchased using a bank account or credit card may be reversed at a later time, for example, if such a payment is subject to a chargeback, reversal, claim or is otherwise invalidated.
- A bitcoin transaction may be unconfirmed for a period of time (usually less than one hour, but up to one day) and never complete if it is in a pending state.
- Holding bitcoin is high risk. The price or value of bitcoin can change rapidly, decrease, and potentially even fall to zero.
- You agree that disputes between you and Coinbase will be resolved by binding, individual arbitration and you waive your right to participate in a class action lawsuit or class-wide arbitration.

1. Our Relationship with You.

1.1 Coinbase helps you make payments to and accept payments from third parties. Coinbase also provides a bitcoin wallet service where you can store your bitcoin. Coinbase also allows users to buy and sell bitcoin. Coinbase is an independent contractor for all purposes. Coinbase does not have control of, or liability for, the products or services that are paid for with Coinbase services. We do not guarantee the identity of any user or other party or ensure that a buyer will complete a transaction. Coinbase is not a money transmitter. Coinbase assists its users in Bitcoin transactions.

1.2 Your Privacy. Protecting your privacy is very important to Coinbase. Please review our [Privacy Policy](#) in order to better understand our commitment to maintaining your privacy, as well as our use and disclosure of your information.

1.3 Privacy of Others; Marketing. If you receive information about another user through Coinbase services, you must keep the information confidential and only use it in connection with Coinbase

services. You may not disclose or distribute a user's information to a third party or use the information for marketing purposes unless you receive the user's express consent to do so. You may not send unsolicited email to a user through Coinbase.

1.4 Intellectual Property. "Coinbase.com", "Coinbase", and all logos related to Coinbase services are either trademarks, or registered marks of Coinbase or its licensors.

1.5 Password Security and Keeping Your Email and Address Current. You are responsible for maintaining adequate security and control of any and all IDs, passwords, personal identification numbers (PINs), or any other codes that you use to access Coinbase services. You are responsible for keeping your email address up to date in your Account Profile.

1.6 Notices to You. You agree that Coinbase may provide you communications about your Account and Coinbase services electronically.

1.7 Notices to Coinbase. We prefer receiving notices to Coinbase electronically through our support system at <http://support.coinbase.com>. Paper notifications can also be sent to Coinbase, Inc., 14525 SW Millikan Way #26680 Beaverton, OR 97005-2343.

2. Accounts.

2.1 Eligibility. To be eligible to use Coinbase services, you must be at least 18 years old (19 in Alabama and Nebraska).

2.2 Identity Authentication. If you wish to buy or sell bitcoin through Coinbase, you authorize Coinbase, directly or through third parties, to make any inquiries we consider necessary to validate your identity.

2.3 Third Party Applications. If you grant express permission to a third party to connect to your Coinbase account, either through the third party's product or through Coinbase, you acknowledge that granting permission to a third party to take specific actions on your behalf does not relieve you of any of your responsibilities under this Agreement. Further, you acknowledge and agree that you will not hold Coinbase responsible for, and will indemnify Coinbase from, any liability arising from the actions or inactions of this third party in connection with the permissions you grant. You may change or remove these permissions at any time from the Account Settings (API) page.

2.4 Taxes. It is your responsibility to determine what, if any, taxes apply to the payments you make or receive, and it is your responsibility to collect, report and remit the correct tax to the appropriate tax authority. Coinbase is not responsible for determining whether taxes apply to your transaction, or for collecting, reporting or remitting any taxes arising from any transaction.

3. Bitcoin.

3.1 Coinbase may cancel or reverse potentially high-risk buys or sells of bitcoin, including those made using reversible payment methods.

3.2 Coinbase does not cancel or reverse bitcoin-to-bitcoin transactions, as long as they are accepted and confirmed on the bitcoin network.

3.3 Coinbase users are in control of their bitcoin at all time, and Coinbase keeps 100% of customer funds in storage. Coinbase does not engage in fractional reserve lending.

3.4 In the event Coinbase needs to retrieve funds from offline storage, there can be a delay in sending coins of up to 48 hours.

3.5 When buying or selling bitcoin, you are buying or selling from Coinbase directly. Coinbase does not act as an intermediary or marketplace between other buyers and sellers of bitcoin.

3.6 Coinbase does not guarantee the value of bitcoin. You acknowledge that the price or value of bitcoin can change rapidly, decrease, and potentially even fall to zero. You acknowledge that holding bitcoin is high risk. You agree to deliver the agreed upon payment for bitcoin upon confirmation of an order, regardless of changes in bitcoin value.

3.7 Coinbase reserves the right to change the buy/sell limits on your account as we deem necessary.

4. Restricted Activities.

4.1 Restricted Activities. In connection with your use of Coinbase services, other users, and third parties you will not:

- Violate any law, statute, ordinance, or regulation (for example, those governing financial services, controlled substances, or consumer protections);
- Intentionally try to defraud Coinbase or other Coinbase users.
- Infringe Coinbase's or any third party's copyright, patent, trademark, or intellectual property rights.
- Provide false, inaccurate or misleading information.
- Take any action that imposes an unreasonable or disproportionately large load on our infrastructure; or detrimentally interfere with, intercept, or expropriate any system, data, or information.

5. Disputes with Coinbase.

5.1 Indemnification. You agree to indemnify and hold Coinbase, its parent, the officers, directors, agents, joint venturers, and employees harmless from any claim or demand (including attorneys' fees) arising out of your breach of this Agreement or your use of Coinbase services.

5.2 Release of Coinbase. If you have a dispute with one or more users, you release Coinbase (and our parent, officers, directors, agents, joint ventures, employees and suppliers) from any and all Claims, demands and damages (actual and consequential) of every kind and nature arising out of or in any way connected with such disputes. In addition, you waive any protection available to you under California Civil Code §1542, which says: [a] general release does not extend to claims which the creditor does not know or suspect to exist in his favor at the time of executing the release, which if not known by him must have materially affected his settlement with the debtor.

5.3 Disputes with Coinbase. If you think we have made an error, write to us at 14525 SW Millikan Way #26680 Beaverton OR, 97005, or email us at support at coinbase.com. In your correspondence, you must give us information sufficient to identify you, your account, and the transaction on which you believe an error occurred. You must contact us within 30 days after the transaction occurred. Within 90 days of receiving your request, we must either correct the error or explain to you why we believe the transaction was correct.

6. General Provisions.

6.1 Limitations of Liability. IN NO EVENT SHALL WE, OUR PARENT, THE OFFICERS, DIRECTORS, AGENTS, JOINT VENTURERS, EMPLOYEES AND SUPPLIERS OF COINBASE OR OUR PARENT BE LIABLE FOR LOST PROFITS OR ANY SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF OR IN CONNECTION WITH OUR WEBSITE, COINBASE SERVICES, OR THIS AGREEMENT (HOWEVER ARISING, INCLUDING NEGLIGENCE). Some states do not allow the

exclusion or limitation of incidental or consequential damages so the above limitation or exclusion may not apply to you. OUR LIABILITY, AND THE LIABILITY OF OUR PARENT, OFFICERS, DIRECTORS, AGENTS, JOINT VENTURERS, EMPLOYEES AND SUPPLIERS, TO YOU OR ANY THIRD PARTIES IN ANY CIRCUMSTANCE IS LIMITED TO THE ACTUAL AMOUNT OF DIRECT DAMAGES.

6.2 No Warranty. COINBASE SERVICES ARE PROVIDED "AS IS" AND WITHOUT ANY REPRESENTATION OF WARRANTY, WHETHER EXPRESS, IMPLIED OR STATUTORY. COINBASE, OUR PARENT, THE OFFICERS, DIRECTORS, AGENTS, JOINT VENTURERS, EMPLOYEES AND SUPPLIERS OF COINBASE OR OUR PARENT SPECIFICALLY DISCLAIM ANY IMPLIED WARRANTIES OF TITLE, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT. Coinbase does not have any control over the products or services that are paid for with Coinbase services and Coinbase cannot ensure that a buyer or a Seller you are dealing with will actually complete the transaction or is authorized to do so. Coinbase does not guarantee continuous, uninterrupted or secure access to any part of Coinbase services, and operation of our site may be interfered with by numerous factors outside of our control. Coinbase will make reasonable efforts to ensure that requests for electronic debits and credits involving bank accounts, credit cards, and check issuances are processed in a timely manner but Coinbase makes no representations or warranties regarding the amount of time needed to complete processing because Coinbase services are dependent upon many factors outside of our control, such as delays in the banking system or the U.S. or international mail service. Some states do not allow the disclaimer of implied warranties, so the foregoing disclaimers may not apply to you. This paragraph gives you specific legal rights and you may also have other legal rights that vary from state to state.

6.3 Arbitration. Except for claims for injunctive or equitable relief or claims regarding intellectual property rights (which may be brought in any competent court without the posting of a bond), any dispute arising under this Agreement shall be finally settled on an individual basis in accordance with the American Arbitration Association's rules for arbitration of consumer-related disputes and you and Coinbase hereby expressly waive trial by jury. The arbitration shall take place in San Francisco, California, in the English language and the arbitral decision may be enforced in any court. The prevailing party in any action or proceeding to enforce this Agreement shall be entitled to costs and attorneys' fees.

6.4 Time Limitation on Claims. You agree that any claim you may have arising out of or related to your relationship with Coinbase must be filed within one year after such claim arose; otherwise, your claim is permanently barred.

PRODUCT

[How To Buy Bitcoin](#)
[Merchant Services](#)
[Developer Platform](#)
[Security](#)

ABOUT

[About](#)
[Careers](#)
[Press](#)
[Legal](#)

RESOURCES

[API](#)
[Documentation](#)
[Status](#)
[Support](#)

FOLLOW US ON

[Our Blog](#)
 [Twitter](#)
 [Facebook](#)

© 2014 Coinbase

coinbase



LEGAL

[USER AGREEMENT](#)[PRIVACY POLICY](#)[LICENSES](#)

PRIVACY POLICY

Last updated: November 17, 2014

Coinbase, Inc. has created the following Privacy Policy to let you know what information we collect when you visit our site, why we collect it and how it is used. This Privacy Policy explains the data collection and use practices of coinbase.com website and mobile apps; it does not apply to other online or offline Coinbase, Inc. sites, products or services. The terms "you," "your," and "yours" refer to the customer/purchaser utilizing our Site. The terms "Coinbase, Inc.," "Coinbase" "we," "us," and "our" refer to Coinbase, Inc. By using this website, you consent to the data practices prescribed in this statement. We may periodically post changes to this Privacy Policy on this page, and it is your responsibility to review this Privacy Policy frequently and we encourage you to visit this page often. When required by law, we will notify you of any changes to this Privacy Policy.

In accordance with our commitment to protect personal privacy, Coinbase adheres to the principles of the U.S.-Swiss Safe Harbor Framework and the U.S.-EU Safe Harbor Framework as developed by the U.S. Department of Commerce in consultation with the European Commission. The seven principles ("Principles") and fifteen Frequently Asked Questions (FAQs) referred to in this policy constitute the Safe Harbor privacy framework. These principles and FAQs may be found at: <http://www.export.gov/safeharbor>.

How we collect information about you

When you visit the Coinbase website, use Coinbase Services, or use third-party services which use the Coinbase

application programming interface ("API"), we collect information sent to us through your computer, mobile phone, or other access device. This information may include your IP address, device information including, but not limited to, identifier, device name and type, operating system, location, mobile network information and standard web log information, such as your browser type, traffic to and from our site and the pages you accessed on our website. You must be at least 18 years old, or of the applicable age of majority, in order to use Coinbase Services. Coinbase does not intentionally collect information from or about any individual who is under 13 years old.

If you create an account or use Coinbase Services, we, or our affiliates vendors acting on our behalf may collect the following types of information:

- Contact information - your name, address, phone, email, Skype ID and other similar information.
- Financial information - the full bank account and routing numbers and/or credit card numbers that you link to your Coinbase Account or input when you use paid Coinbase Services. If you do not use the Coinbase Conversion Service, you may opt out of providing this information.

If you seek permissions to raise bitcoin buy and sell limits associated with your Coinbase Account, we may require you to provide additional information which we may use in collaboration with service providers acting on our behalf to verify your identity or address, and/or to manage risk. This information may include your date of birth, taxpayer or government identification number, a copy of your government-issued identification, or other personal information. We may also obtain information about you from third parties such as credit bureaus and identity verification services. If you do not use the Coinbase Conversion Service, you may opt out of providing this additional information.

When you use Coinbase Services, we collect information about your transactions and/or your other activities on our website and we may continuously collect information about your computer, mobile device, or other access device for fraud prevention purposes, to monitor for possible breach of your Coinbase Account, and to identify any malicious software or other activity that may harm Coinbase or its users.

You may choose to provide us with access to certain personal information stored by third parties such as social media sites (such as Facebook and Twitter). The information we have access to varies by site and is controlled by your privacy settings on that site and your authorization. By associating an account managed by a third party with your Coinbase account and authorizing Coinbase to have access to this information, you agree that Coinbase may collect, store and use this information in accordance with this Privacy Policy.

Finally, we may collect additional information you may disclose to our customer support team.

How we use cookies

When you access our website or content or use our application or Coinbase Services, we or companies we work with may place small data files called cookies or pixel tags on your computer or other device. We use these technologies to:

- Recognize you as a Coinbase customer;

- Customize Coinbase Services, content, and advertising;
- Measure promotional effectiveness; and
- Collect information about your computer or other access device to mitigate risk, help prevent fraud and promote trust and safety.

We use both session and persistent cookies when you access our website or content. Session cookies expire and no longer have any effect when you log out of your account or close your browser. Persistent cookies remain on your browser until you erase them or they expire.

We also use Local Shared Objects, commonly referred to as "Flash cookies," to help ensure that your account security is not compromised, to spot irregularities in behavior to help prevent fraud and to support our sites and services.

We encode our cookies so that only we can interpret the information stored in them. You are free to decline our cookies if your browser or browser add-on permits, but doing so may interfere with your use of our website. The help section of most browsers or browser add-ons provides instructions on blocking, deleting or disabling cookies.

You may encounter Coinbase cookies or pixel tags on websites that we do not control. For example, if you view a web page created by a third party or use an application developed by a third party, there may be a cookie or pixel tag placed by the web page or application. Likewise, these third parties may place cookies or pixel tags that are not subject to our control and the Coinbase Privacy Policy does not cover their use.

How we protect and store personal information

Throughout this policy, we use the term "personal information" to describe information that can be associated with a specific person and can be used to identify that person. We do not consider personal information to include information that has been anonymized so that it does not identify a specific user. Coinbase takes reasonable precautions, as described herein, to protect your personal information from loss, misuse, unauthorized access, disclosure, alteration, and destruction.

We store and process your personal and transactional information, including certain payment information, such as your encrypted bank account and/or routing numbers, on our computers in the United States and elsewhere in the world where Coinbase facilities or our service providers are located, and we protect it by maintaining physical, electronic and procedural safeguards in compliance with applicable US federal and state regulations. We use computer safeguards such as firewalls and data encryption, we enforce physical access controls to our buildings and files, and we authorize access to personal information only for those employees who require it to fulfill their job responsibilities. Full credit card data is securely transferred and hosted off-site by a payment vendor in compliance with Payment Card Industry Data Security Standards (PCI DSS). This information is not accessible to Coinbase staff.

We store our customers' personal information securely throughout the life of the customer's Coinbase Account. Coinbase will retain your personal information for a minimum of five years or as necessary to comply with our legal obligations or resolve disputes.

How we use the personal information we collect

Our primary purpose in collecting personal information is to provide you with a secure, smooth, efficient, and customized experience. We may use your personal information to:

- Provide Coinbase Services and customer support you request;
- Process transactions and send notices about your transactions;
- Resolve disputes, collect fees, and troubleshoot problems;
- Prevent and investigate potentially prohibited or illegal activities, and/or violations of our posted user terms;
- Customize, measure, and improve Coinbase Services and the content and layout of our website and applications;
- Deliver targeted marketing, service update notices, and promotional offers based on your communication preferences; and
- Compare information for accuracy and verify it with third parties.

We will not use your personal information for purposes other than those purposes we have disclosed to you, without your permission. From time to time we may request your permission to allow us to share your personal information with third parties. You may opt out of having your personal information shared with third parties, or from allowing us to use your personal information for any purpose that is incompatible with the purposes for which we originally collected it or subsequently obtained your authorization. If you choose to so limit the use of your personal information, certain features or Coinbase Services may not be available to you.

Marketing

We will not sell or rent your personal information to third parties for their marketing purposes without your explicit consent. We may combine your information with information we collect from other companies and use it to improve and personalize Coinbase Services, content and advertising.

How personal information is shared with other Coinbase users

To process your payments, we may share some of your personal information with the person or company to which you transfer or from which you receive bitcoin. Your contact information, date of sign-up, the number of payments you have received from verified Coinbase users, and whether you have verified control of a bank account are provided to other Coinbase users with whom you transact through Coinbase. In addition, this and other information you disclose to Coinbase may be shared with third parties who may provide, upon your authorization, ancillary services which access your Coinbase Account. Unless you have agreed to it, these third parties are not allowed to use this information for any purpose other than to facilitate your transactions using Coinbase services.

If you use your Coinbase Account to transfer bitcoin in connection with the purchase or sale of goods or services, we or you may also provide the seller with your shipping address to help complete your transaction with the seller. The seller is not allowed to use this information to market their services to you unless you have agreed to it. If an attempt to transfer bitcoin to your seller fails or is later invalidated, we may also provide your seller with details of the unsuccessful transfer. To facilitate dispute resolutions, we may provide a buyer with the seller's address so that goods can be returned to the seller.

In connection with a bitcoin transfer between you and a third party, including merchants, a third party may share information about you with us, such as your email address or mobile phone number which may be used to inform you that a transfer has been sent to or received from the third party. We may use this information in connection with such transfers to confirm that you are a Coinbase customer, that bitcoin transfers are enabled, and/or to notify you that you have received bitcoin. If you request that we validate your status as a Coinbase customer with a third party, we will do so. You may also choose to send bitcoin to or request bitcoin from an e-mail address. In such cases, your user name will be displayed in an e-mail message notifying the user of the designated e-mail address of your action. Please note that merchants you interact with may have their own privacy policies, and Coinbase is not responsible for their operations, including, but not limited to, their information practices.

How we share personal information with other parties

We may share your personal information with:

- Service providers under contract who help with parts of our business operations such as fraud prevention, bill collection, marketing and technology services. Our contracts dictate that these service providers only use your information in connection with the services they perform for us and not for their own benefit.
- Financial institutions with which we partner.
- Companies that we plan to merge with or be acquired by. (Should such a combination occur, we will require that the new combined entity follow this Privacy Policy with respect to your personal information. You will receive prior notice of any change in applicable policy.)
- Law enforcement, government officials, or other third parties when:
 - We are compelled to do so by a subpoena, court order or similar legal procedure; or
 - We believe in good faith that the disclosure of personal information is necessary to prevent physical harm or financial loss, to report suspected illegal activity or to investigate violations of our User Agreement.
- Other third parties with your consent or direction to do so.

Coinbase will not sell or rent any of your personal information to third parties for their marketing purposes and only shares your personal information with third parties as described in this policy. Before Coinbase shares your information with any third party that is not acting as an agent to perform tasks on behalf of and under the instructions of Coinbase, Coinbase will first ensure that the third party either subscribes to the Principles, or is subject to the European Union's Directive on Data Protection, or enters into a written agreement with Coinbase requiring that the third party will provide at least the same level of privacy protection as required by the Principles.

If you establish a Coinbase account indirectly on a third party website or via a third party application, any information that you enter on that website or application (and not directly on a Coinbase website) will be shared

with the owner of the third party website or application and your information may be subject to their privacy policies.

In general, we will notify you of material changes to this policy by updating the last updated date at the top of this page, and we will provide you with explicit notice of material changes as required by law. We recommend that you visit this page frequently to check for changes.

How you can access or change your personal information

You are entitled to review, correct, or amend your personal information, or to delete that information where it is inaccurate, and you may do so at any time by logging in to your account and clicking the Profile or My Account tab. This right shall only be limited where the burden or expense of providing access would be disproportionate to the risks to your privacy in the case in question, or where the rights of persons other than you would be violated. If you close your Coinbase account, we will mark your account in our database as "Closed," but will keep your account information in our database for a period of time described above. This is necessary in order to deter fraud, by ensuring that persons who try to commit fraud will not be able to avoid detection simply by closing their account and opening a new account. However, if you close your account, your personally identifiable information will not be used by us for any further purposes, nor sold or shared with third parties, except as necessary to prevent fraud and assist law enforcement, as required by law, or in accordance with this Privacy Policy.

How you can contact us about privacy questions

If you have questions or concerns regarding this policy, you should contact us on our [support page](#) or by writing to us at Coinbase, Inc. 548 Market Street #23008 San Francisco, CA 94104, USA. If you believe your privacy has been compromised as a result of your use of Coinbase Services, you may submit a complaint through our independent data privacy consultant, Privacy Trust, [via this form](#).





© 2015 Coinbase

PRODUCTS

[Bitcoin Wallet](#)

[Merchant Tools](#)

[Developer](#)

[Platform](#)

[Exchange](#)

[Vault](#)

[Mobile](#)

[App Gallery](#)

RESOURCES

[What is bitcoin?](#)

[Buy Bitcoin](#)

[Help](#)

[Charts](#)

[Security](#)

[Global](#)

[Status](#)

ABOUT

[About](#)

[Careers](#)

[Mission](#)

[Press](#)

[Legal & Privacy](#)

SOCIAL

[Our Blog](#)

[Community](#)

[Twitter](#)

[Facebook](#)

LANGUAGE

[English](#)

[Help translate](#)

[Coinbase](#)



[INVEST IN BITCOIN](#) [BUY BITCOIN WITH CREDIT CARD](#) [BLOG](#)

[BIT10 INDEX TOKEN](#)

Last updated: October 16, 2018

By visiting, accessing, or using Abra, you consent to the policies and practices of our privacy policy (the “Privacy Policy”) so please read them carefully. If any policies or practices described in this Privacy Policy are unacceptable to you, please do not visit, access, or use Abra. Use of the words “we,” “us,” or “our” in this Privacy Policy refers to Plutus Financial, Inc. (d/b/a Abra) and any or all of its affiliates.

PRIVACY POLICY

INTRODUCTION

At Abra, your trust is one of our most important assets. We continually work to protect the privacy of our users and continually review our Privacy Policy. This website will always contain the most current Privacy Policy. If we decide to change our privacy practices, we will post those changes to this Privacy Policy and other places we deem appropriate so that you are aware of what information we collect, how we use it, and under what circumstances, if any, disclose it. We reserve the right to modify this Privacy Policy at any time, so please review it frequently. If we change how we use your Personal Information (as defined below), we will notify you here, by email, or by means of a notice on our home page.

PERSONAL INFORMATION

As used herein, “Personal Information” means any information relating to an identified or identifiable natural person (each, a “Data Subject”); an identifiable natural person is one who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, or an online identifier or to one or more factors specific to the physical, economic, cultural or social identity of that natural person.

PERSONAL INFORMATION WE COLLECT

The USA PATRIOT ACT requires all financial institutions to obtain, verify, and record Personal Information that identifies each person who opens an account. This federal requirement applies to all new users. This Personal Information is used to assist the United States government in the fight

against the funding of terrorism and money-laundering activities. What this means for you: when you create an Abra Wallet, we ask you for your name, email address, mobile phone number and other identifying Personal Information.

Personal Information we collect may include the following:

Individual Users — Depending on your level of activity, Abra will attempt to collect, verify, and authenticate the following:

- Email address;
- Mobile phone number;
- Full legal name;
- Social Security Number (“SSN”) or a comparable government-issued identification number;
- Date of birth;
- Proof of identity (e.g., unexpired driver’s license, passport or other government-issued identification);
- Home address (not a mailing address or P.O. Box); and
- Additional Personal Information or documentation at the discretion of our Operations Staff.

Legal Entities — We attempt to collect, verify, and authenticate the following:

- Entity legal name;
- Employer Identification Number (“EIN”) or any comparable identification number issued by a government;
- Full legal name of all account signatories;
- Email address of all account signatories;
- Mobile phone number of all account signatories;
- Principal place of business and/or other physical location;
- Proof of legal existence (e.g., state certified articles of incorporation or certificate of formation, unexpired government-issued business license, trust instrument, or other comparable legal documents as applicable); and
- Documentation indicating that the signatories are authorized to act on behalf of the legal entity.

Device Information – Information automatically collected about the device used to access the Abra platform (such as, but not limited to, hardware, operating system, browser, etc.).

Location Information – Information automatically collected to determine your location, including your IP address and/or domain name.

Log Information – Information that is generated by your use of Abra that is automatically collected and stored in our server logs. This may include, but is not limited to, device-specific information, location

information, system activity and any information related to Abra services you utilize.

Transactional Information – Information that is generated by your activity, including, but not limited to, trading activity, order activity, deposits, withdrawals, and wallet balances.

Correspondence – Information that you provide to us in correspondence, including creating a wallet or wallets, and with respect to ongoing user support.

COOKIES

Some of our web pages may contain “cookies”, or data that is sent to your web browser and stored on your computer. The purpose of these “cookies” is to allow our server to recognize you as a returning visitor, customize our services, content, and advertising; measure promotional effectiveness; help ensure that your account security is not compromised; mitigate risk and prevent fraud; and to promote trust and safety across our sites and services. We may also use trusted third-party services that track this information on our behalf. In the event you do not wish to receive such cookies, you may configure your web browser to not accept cookies or to notify you if a cookie is sent to you. You are free to decline cookies if your web browser permits, but you may not be able to use all the features and functionalities of our website. Abra does not link the information we store in cookies to any personally identifiable information you submit while on our website.

HOW WE USE AND SHARE THE PERSONAL INFORMATION WE COLLECT

The Personal Information we collect and the practices described above are done in an effort to provide you with the best experience possible, protect you from risks related to improper use and fraud, and help us maintain and improve the Abra platform.

We may share Personal Information with third-party service providers (including those that may be located outside of the United States or your country), who help us operate our platform and systems, and detect fraud and security threats during the normal course of our business. Such third-party service providers are subject to strict confidentiality obligations.

For example, we may use your Personal Information to:

Provide you with our services, including user support for Abra;

- Optimize and enhance our services for all users or for you specifically;
- Conduct anti-fraud and identity verification and authentication checks (you authorize us to share your Personal Information with our third-party service providers, who may also conduct their own searches of publicly available Personal Information about you);
- Monitor the usage of our services, and conduct automated and manual security checks of our services; and

- Create aggregated and anonymized reporting data about our services.

If we decide to modify the purpose for which your Personal Information is collected and used, we will amend this Privacy Policy.

If we propose to sell or buy any business or assets, we may disclose your Personal Information in an anonymized form to the prospective buyer or seller of such business or assets. In the event of a merger, acquisition, or asset sale of Abra, we will give you notice if, and before, your Personal Information is transferred in a non-anonymized form or becomes subject to a different privacy policy.

Abra may, under certain circumstances and in its sole discretion, disclose your information if we believe that it is reasonable to do so. Such disclosure or transfer is limited to situations where the personal data are required for the purposes of (1) provision of the services, (2) pursuing our legitimate interests, (3) law enforcement purposes, or (4) if you provide your prior explicit consent.

Such reasonable disclosure cases may include, but are not limited to:

- Satisfying any local, state, or Federal laws or regulations;
- Responding to requests, such as discovery, criminal, civil, or administrative process, subpoenas, court orders, or writs from law enforcement or other governmental or legal bodies;
- Bringing legal action against a user who has violated the law or violated our Terms of Use;
- As may be necessary for the operation of Abra;
- Generally cooperating with any lawful investigation about our users; or
- If we suspect any fraudulent activity or have noticed any activity which may violate our Terms of Use or other applicable rules.

Be aware that Bitcoin, Litecoin, and other cryptocurrencies are not necessarily anonymous. Generally, anyone can see the balance and transaction history of any public cryptocurrency address. We, and any others who can match your public cryptocurrency address to other Personal Information about you, may be able to identify you from a blockchain transaction. This is because, in some circumstances, Personal Information published on a blockchain (such as your cryptocurrency address and IP address) can be correlated with Personal Information that we and others may have. This may be the case even if we, or they, were not involved in the blockchain transaction. Furthermore, by using data analysis techniques on a given blockchain, it may be possible to identify other Personal Information about you. As part of our security, anti-fraud and/or identity verification and authentication checks, we may conduct such analysis to collect and process such Personal Information about you. You agree to allow us to perform such operations and understand that we may do so.

DATA SECURITY

Protection of Personal Data

We take the protection and storage of your personal data very seriously and take all reasonable steps to ensure the ongoing confidentiality, integrity, and availability of your personal data. We protect your personal data by using reasonable security safeguards against loss or theft, unauthorized access, disclosure, copying, use, or modification. Your personal data is stored behind secured networks and is accessible by a limited number of persons who have special access rights to such systems and are required to keep the personal data confidential. We implement a variety of security measures, such as encryption and anonymization when users enter, submit, or access their personal data to maintain the safety of their personal data. Please note, however, that no system involving the transmission of information via the Internet, or the electronic storage of data, is completely secure. Consequently, we are not liable for any loss, theft, unauthorized access, disclosure, copying, use, or modification of your personal data that occurs outside our reasonable control.

Breach notification

Should a personal data breach occur, we will inform the relevant authorities without undue delay and immediately take reasonable measures to mitigate the breach. We will notify you about such a breach via email as soon as possible but no later than within seven business days.

ACCURACY AND RETENTION OF PERSONAL INFORMATION

We take reasonable and practicable steps to ensure that your Personal Information held by us (i) is accurate with regard to the purposes for which it is to be used, and (ii) is not kept longer than is necessary for the fulfillment of the purpose for which it is to be used, which is when your business relationship with us ends, unless the further retention of your Personal Information is otherwise permitted or required by applicable laws and regulations.

ACCESS, CORRECTION, AND DELETION OF PERSONAL INFORMATION

You have the right to ascertain whether we hold your accurate and current Personal Information, to obtain a copy of the Personal Information that you submitted as permitted by law, and to correct any of your data that is inaccurate. You may also request that we inform you of the type of Personal Information we hold with regard to you, subject to restrictions on our providing copies of certain data pursuant to our obligations under the Bank Secrecy Act ("BSA") and Anti-Money Laundering ("AML") regulations and/or data provided to our legal counsel in defense of a claim against us. You may also request that we delete your Personal Information, subject to restrictions under applicable laws and regulations, such as those related to the BSA and AML. For data access, correction, or deletion requests, please contact privacy@abra.com.

When handling a data access, correction, or deletion request, we check the identity of the requesting party to ensure that he or she is the person legally entitled to make such request. While our policy is to respond to such requests free of charge, we reserve the right to charge you a reasonable fee for compliance with your request should your request be repetitive or unduly onerous.

DIRECT MARKETING

Subject to applicable laws and regulations, we may from time to time send direct marketing materials promoting services, products, facilities, or activities to you using information collected from you. We will provide you with an opportunity to opt-out of such communications and will only send them to you if you consent.

We do not sell user Personal Information to third parties for the purpose of marketing.

EU-U.S. PRIVACY SHIELD AND SWISS-U.S. PRIVACY SHIELD

As a global entity, Abra may store, transfer, and otherwise process your personal information in countries outside of the country of your residence, including the United States and possibly other countries.

Abra complies with the *EU-U.S. Privacy Shield Framework and/or the Swiss-U.S. Privacy Shield Frameworks*, as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from the *European Union and Switzerland* to the United States. Abra has certified to the Department of Commerce that it adheres to the Privacy Shield Principles. If there is any conflict between the terms in this Privacy Policy and the Privacy Shield Principles, the Privacy Shield Principles shall govern. To learn more about the Privacy Shield program, and to view our certification, please visit <https://www.privacyshield.gov/>.

Abra is responsible for the processing of personal information it receives under the Privacy Shield Framework and subsequently transfers to a third party acting as an agent on its behalf. Pursuant to the Privacy Shield Principles, Abra will use personal information only in ways that are compatible with the purposes for which it was collected or subsequently authorized by the individual. We take all reasonable steps to ensure that personal information we process is limited to only what is relevant to the purposes for which it was collected and that it is accurate, complete, and up-to-date.

Abra complies with the Privacy Shield Principles for all onward transfers of personal information from the EU and/or Switzerland, including the onward transfer liability provisions. Consequently, before Abra shares your information with any third party that is not also certified under the EU-U.S. Privacy Shield and/or the Swiss-U.S. Privacy Shield Frameworks, Abra will enter into a written agreement that the third party provides at least the same level of privacy safeguard as required under those Frameworks, and assures the same level of protection for the personal information as required under applicable data protection laws.

COMPLAINTS ABOUT HANDLING OF PERSONAL DATA

Abra commits to resolve European and/or Swiss data subjects' complaints about their privacy and our collection, use or disclosure of their personal information in compliance with the EU-U.S. Privacy Shield and/or the Swiss-U.S. Privacy Shield Principles. You have the right to submit a complaint to us about the way in which your personal data have been handled by using the contact details indicated in the "Contact Us" section of this Privacy Policy.

After you submit such a complaint, we will send you an email within five business days confirming that we have received your complaint. Afterwards, we will investigate your complaint and provide you with our response within a reasonable timeframe.

If you are a European and/or Swiss Data Subject with an unresolved complaint or dispute arising under the requirements of the Privacy Shield Frameworks, you may refer your complaint under the Frameworks to an independent dispute resolution mechanism, free of charge to you. Our independent dispute resolution mechanism is JAMS Mediation, Arbitration and ADR Services (“JAMS”). You may contact JAMS at <https://www.jamsadr.com/eu-us-privacy-shield>.

We are also subject to the investigatory and enforcement powers of the U.S. Federal Trade Commission with respect to the Framework. Please note that under limited circumstances, a binding arbitration option may be available before a Privacy Shield Panel if your complaint is not resolved through the mechanisms describes above.

If you are a resident of the European Union and you are not satisfied with the outcome of your complaint, you have the right to lodge a complaint with your local data protection authority.

CONTACT US

If you are located in the EU or Switzerland and have questions or concerns regarding the processing of your Personal Information, you may contact us at: privacy@abra.com or write us at:

Plutus Financial, Inc.
PO Box 390004
Mountain View, CA 94039
USA

Get the app for free



SEND ME A LINK

You will receive a one-time text message to download the app.
Carrier charges may apply.



COMPANY

- [About Us](#)
- [Jobs](#)
- [Press](#)
- [Contact Us](#)
- [Blog](#)

LEARN MORE

- [Where is Abra Available?](#)
- [Fees](#)
- [FAQ](#)
- [Become a Partner](#)
- [Affiliates](#)
- [Sitemap](#)

INVEST IN BITCOIN

- [All About Bitcoin](#)
- [What is Bitcoin?](#)
- [How Does Bitcoin Work?](#)
- [Where to Buy Bitcoin](#)
- [Buy Bitcoin with Abra](#)

INVEST IN CRYPTOS

- [Invest in Crypto](#)
- [Ethereum](#)
- [Ultimate Altcoin Guide](#)

OUR TECHNOLOGY

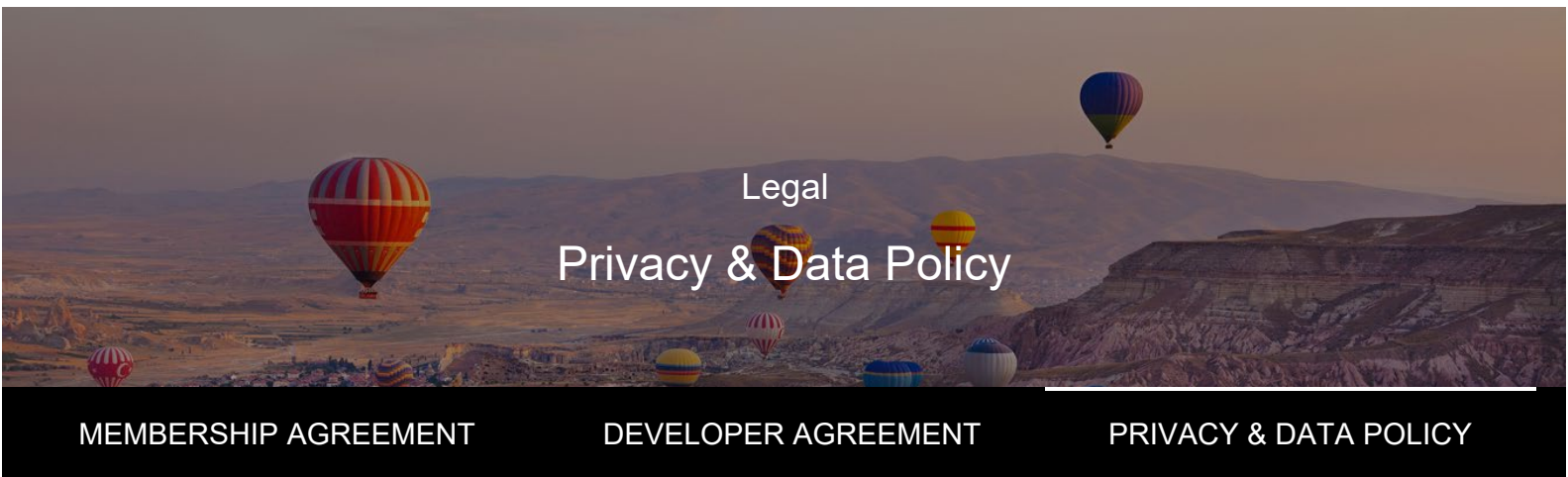
- [How it Works](#)
- [Safety](#)

Copyright 2018 Plutus Financial, Inc. All rights reserved. [Privacy Policy](#). [Terms of Service](#).





transparency-assettransparency-averagetransparency-obligationstransparency-reservetransparency-
 volumecountries-worldstatus-downstatus-goodstatus-minorfeatures-computerfeatures-connectionfeatures-
 devicefeatures-scamsfeatures-getting-startedfeatures-hackfeatures-insurancefeatures-vacationsfeatures-
 ownershipfeatures-2fafeatures-memberfeatures-passwordfeatures-collaborativefeatures-commitedfeatures-
 compassionfeatures-consciousfeatures-creativefeatures-curiousfeatures-leadfeatures-tenaciousfeatures-
 donationsfeatures-bankfeatures-credit-cardfeatures-infofeatures-rewardfeatures-withdrawfeatures-
 communitytransparency-transactionscountries-chinacountries-europecountries-usafeatures-apifeatures-
 blogcheckedcarousel-arrow-nextcarousel-arrow-prevfeatures-accessfeatures-auditingfeatures-
 diligencefeatures-personnelfeatures-securityfeatures-freefeatures-globalfeatures-innovativefeatures-
 transparencypercent-0percent-5offices-bragaoffices-londonoffices-san-franciscooffices-shanghaifeatures-
 assurancefeatures-convertfeatures-fundfeatures-holdfeatures-movefeatures-
 secureglobersstwitterfacebookemailinstagramlinkedinchevron-rightchevronclose-circleclosecurrency-
 btccurrency-cnycurrency-eurcurrency-gbpcurrency-jpycurrency-usdlocationmagnifyobligationssafeshare-
 circlesharetransactiontwitter-favoritetwitter-moretwitter-replytwitter-retweet



COOKIE POLICY

Our Commitment To Privacy

At Uphold, we understand how important privacy is to our members and partners. That’s why we are committed to maintaining the confidentiality, integrity, and security of all personal information. We collect only what we need in order to provide a secure service, and we don’t share your personal information with any third parties except to ensure the safety, quality and certain aspects of our service, compliance with laws and regulations, and the security of you, our members and our partners. When we do share your information with third parties, we work to ensure that they only use it for the contracted purposes and that they keep it secure. Within Uphold, access to your personal information is limited to those people who need it to do their jobs, consisting generally of our legal,

compliance, product and identity verification professionals.



Protecting Your Personal Information is Our Default Mode

Unless disclosure is required by rare circumstances, we work hard to keep your personal information private.



We Keep Your Personal Information Safe

There is no way to eliminate all risk, but we are dedicated to keeping your personal information safe.



Real-time Transparency and Personal Privacy are Compatible

Our real-time public transparency and proof of solvency do not reveal your personal information.

UPHOLD PRIVACY & DATA POLICY

Last updated on October 14, 2015.

1. PURPOSE OF THIS PRIVACY & DATA POLICY

Uphold HQ, Inc., a company incorporated under the laws of South Carolina, Uphold Worldwide Ltd., incorporated under the laws of Antigua, W.I. and related companies and affiliates have created the following Privacy & Data Policy to let you know what information we collect when you visit our websites, use our products, services, or apps (our "Service"), or access and/or use third-party services that use our Application Programming Interface ("API"), why we collect such information, and how it may be used.

We may periodically post changes to this Privacy and Data Policy on this page, and trust you will review the content regularly We may also notify you of changes by email or through other communication channels.

2. HOW WE COLLECT INFORMATION ABOUT YOU

2.1 We collect information from and about you when you register or use our Service. When registering you may be asked for detailed information including your name, email address, physical mailing address, phone number, government issued identification documents, or other information. We may also request and receive information about you from other sources or use other sources to confirm the

information that you provide us.

2.2 When you visit our site and/or use our Service, we automatically collect information sent to us by your computer, mobile phone, or other device. This information may include your IP address, device information (including, but not limited to, identifier, name and type, operating system, mobile network information), standard web log information, such as your browser type, and the pages you access on our site.

2.3 When you use a location-enabled device with our Service, we may collect geographical location data or use various means to determine your location, such as sensor data from your device that may, for instance, provide data on nearby cell towers and Wi-Fi access spots.

2.4 We may log information using “cookies.” Cookies are small data files stored on your hard drive by a website. Cookies help us make our site and Service and your use of them better by allowing us to recognize your browser and capture and remember certain information. Please see our [Cookie Policy](#) for additional information.

3. REGARDING CHILDREN’S PRIVACY

You must be at least 18 years old, or at least 13 years old under the direct supervision of your parent or guardian, to use the Service. We do not knowingly solicit or collect information from individuals under 13. If we become aware that a child under the age of 13 has provided us with personal information, we will delete that information.

4. HOW WE USE YOUR PERSONAL INFORMATION

4.1 We use your personal information to: (i) operate, maintain, and improve our Service; (ii) respond to comments and questions and provide support to our Members; (iii) send information including confirmations, invoices, technical notices, updates, security alerts, and support and administrative messages; (iv) communicate about promotions, upcoming events, and other news about products and services offered by us or any affiliates; (v) link or combine member information with other personal information; (vi) protect, investigate, and deter against fraudulent, unauthorized, or illegal activity; and (vii) provide and deliver the Service.

4.2 If you register for or use Service, we, or our affiliates, partners and/or vendors acting on our behalf, may collect the following types of information:

- Contact information: your name, address, phone, email, Skype ID and other similar information;
- Identity Verification Information: We may require you to provide additional information that we may use and provide to partners and or vendors acting on our behalf to verify your identity. This information may include your date of birth, taxpayer or government identification number, a copy of your government-issued identification, or other personal information. We may also obtain information about you from third parties such as credit bureaus and identity verification services;

- Ongoing Information Collection: When you use our Service, we collect information about your transactions and/or your other activities on our site or Service and we may continuously collect information about your computer, mobile device, or other access device to protect the Service, members and us, for fraud prevention and remediation purposes, to monitor for irregular activity with your account, and to identify known malicious software or other activity that may harm us or our members;
- Social Media-Related Information: You may choose to provide us with access to certain personal information stored by third parties such as social media sites (like Facebook, Google, Twitter, etc). The information we have access to varies by site and is controlled by you. If you associate an account managed by a third party with your Uphold account you authorize us to have access to and use this information; and
- If you authorize applications or third party integrations on or using our Service, these parties may receive detailed information about your account, your use of the Service, transaction history or even the ability to take actions on your behalf. Information collected by these applications or third-party integrations are subject to their terms and policies.

4.3 We may also collect additional information you may disclose to our member support team in order to resolve problems you report.

5. HOW WE SAFEGUARD YOUR PERSONAL INFORMATION

5.1 We use the term "personal information" to describe information that can be associated with a specific person and can be used to identify that person. We do not consider personal information to include information that has been anonymized so that it does not identify a specific user. We take carefully considered and periodically reviewed measures, as described herein, to protect your personal information.

5.2 We store and process your personal and transactional information on our servers in the United States and elsewhere in the world where we, our affiliates, our partners, providers or vendors are located, and we protect that information by maintaining physical, electronic, and procedural safeguards, incorporating tested security technologies, in compliance with applicable laws. We may use network safeguards such as firewalls and data encryption, enforce physical access controls, and authorize access to personal information only for those people who require access to fulfill their job responsibilities. Those with access to your personal information are carefully screened, periodically reevaluated, and are required to keep all member personal information confidential. Security risks exist and no organization can genuinely promise you otherwise. Bad actors may defeat even the most carefully considered and implemented safeguards.

5.3 We store personal information securely and will retain that information for as long as necessary to maintain the Service, comply with our legal obligations and/or resolve disputes.

6. WHAT UPHOLD'S REAL-TIME PUBLIC TRANSPARENCY REVEALS ABOUT YOUR TRANSACTIONS:

6.1 We publish a real-time accounting of all movements of value into, within, and out of our system via our Reservechain™. The Reservechain™ does not contain any personal information. However, the amount, asset class, and time-stamp of all transactions conducted using our Service is publicly available on the Reservechain™ and that information is a permanent part of the publicly-accessible Reservechain™. The Reservechain™ does not contain information that is directly attributable to any Members who are not a party to the transaction. Only members who are party to the transaction have the ability to access personally identifiable information associated with their transactions.

6.2 We publish a real-time accounting of all movements of our financial obligations to our members, our solvency as well as a real-time accounting of all movements of value in the reserve of assets that substantiates the value of assets enabled by our system. This Reserveledger™ contains no personal information. However, the amount, asset class, and time-stamp of all transactions conducted using our Service are publicly reported on the Reserveledger™ and that information is a permanent part of the publicly-accessible Reserveledger™. The Reserveledger™ does not contain information that is directly attributable to any members who are not a part of a given transaction. Only members who are party to the transaction have the ability to access personally identifiable information associated with their transactions..

7. SHARING YOUR PERSONAL INFORMATION

7.1 We do not sell, trade, or otherwise transfer to outside parties your personal information. This does not include third parties who assist us in operating our Service, conducting our business, or supporting our members, so long as those parties agree to keep this information confidential and secure and on the same conditions and protection levels we provide to you as a member. Our agreements with third parties that have access to your personal information generally oblige them to keep your personal information secure and to delete your personal information when access is no longer required. We periodically review the security and confidentiality practices of third parties who we entrust with your personal information. We may also release your information to certified and authorized law enforcement officials when we believe release is appropriate to comply with the law, enforce our terms or policies, or protect the rights, property, or safety of Uphold, our members, or others. We have a set of guidelines for how we engage with law enforcement officials that is available to the public [here](#).

7.2 We may share your personal information as follows:

- With your consent;
- To comply with applicable laws;
- To respond to governmental requests and legal process;
- To protect our rights, the rights of our affiliates, partners or vendors, the rights of other members,

or others. This includes, without limitation, disclosures we may need to make to enforce our agreements, terms and policies;

- In an emergency. This includes protecting the safety of our employees and agents, our members, or others;
- To certain employees, affiliates and vendors when necessary for their roles; and
- If applicable, with entities that we may merge with or be acquired by. (Should such a combination occur, we will require that the new combined entity follow this Policy with respect to your personal information and will provide you with notice of any material changes).

8. MARKETING COMMUNICATIONS

Our marketing emails and other electronic communications tell you how to “opt-out” of receiving more of the same. If you opt-out, we may still send you non-marketing emails and other electronic communications. Non-marketing emails or other electronic communications include emails about your account, transactions, and other aspects of our of site or Service. You may send requests about your personal information to our support teams below where you can request to change contact choices, opt-out of our sharing with others, and update your personal information.

9. CONTACT INFORMATION

If there are any questions regarding this Privacy & Data Policy you may contact us using the information below.

Contact us online.

Addresses:

Uphold HQ, Inc.

1703 Laurel Street

Columbia, SC 29201

United States of America

Uphold Worldwide Ltd.

Unit #3B,

Bryson's Commercial Complex, Friars Hill Road,

St. John's,

Antigua, W.I.

Go

JUN

SEP

NOV

◀ 01 ▶

2018

2019

2020

[11 captures](#)

21 Jan 2016 - 29 Nov 2019

▼ About this capture

Help

For Law Enforcers

INFORMATION AND GUIDELINES FOR AUTHORIZED LAW ENFORCEMENT OFFICIALS WITH THE LEGAL AUTHORITY TO MAKE REQUESTS:

Upholding the integrity of our platform and protecting our members and their personal information is of the utmost importance to Uphold. Authorized law enforcement officials, with the legal authority to make requests for information, should follow these guidelines, as detailed below.

If you are a private party engaged in litigation, requests for information should be directed to the parties to that litigation. Members seeking information on their own accounts may collect — or have their attorneys collect — information directly from their accounts. This information is for guidance only and is subject to change.

HOW TO ENGAGE AND CONTACT UPHOLD IF YOU ARE AN AUTHORIZED LAW ENFORCEMENT OFFICIAL WITH THE LEGAL AUTHORITY TO MAKE REQUESTS.

Last updated on October 14, 2015.

1. MAKING CONTACT WITH UPHOLD & REQUESTS FOR INFORMATION

<https://uphold.com/en/help/for-law-enforcers>

Go

JUN

SEP

NOV

◀ 01 ▶

2018

2019

2020



▼ About this capture

11 captures

21 Jan 2016 - 29 Nov 2019

1.1 Proof of authority to request information, including the name of the issuing authority;

- A. The badge and ID number of responsible agent;
- B. The email address from a government domain; and
- C. A direct contact number at the requesting governmental agency.

2. UNITED STATES LAW ENFORCEMENT

We disclose records in accordance with our Membership Agreement and applicable law, including the federal Stored Communications Act (“SCA”), 18 U.S.C. § 2701 et seq.

- A. We require a valid subpoena issued in connection with an official criminal investigation for the disclosure of basic subscriber records (defined in 18 U.S.C. § 2703(c)(2)), which may include: name, length of service, credit card information, email address(es), and recent IP address(es), if available.
- B. We require a court order issued under 18 U.S.C. § 2703(d) for the disclosure of certain records or other information pertaining to the account, not including any contents of communications, which may include message headers and IP addresses, in addition to the basic subscriber records identified above.
- C. We require a search warrant issued under the procedures described in the Federal Rules of Criminal Procedure or equivalent state warrant procedures upon a showing of probable cause for the disclosure of any stored content, which may include available messages sent with a transfer, if any.
- D. We interpret the national security letter provision as applied to us to require the production of only: name and length of service.

3. INTERNATIONAL LAW ENFORCEMENT

We disclose account records solely in accordance with our terms, policies and applicable law. A Mutual Legal Assistance Treaty request or letters rogatory may be required to compel the disclosure of information.

4. ACCOUNT PRESERVATION

We will take steps to preserve records in connection with official investigations for 90 days pending receipt of formal legal process. You may submit formal preservation requests by email to compliance@uphold.com, mail or recognized courier service.

https://uphold.com/en/help/for-law-enforcers JUN SEP NOV
◀ 01 ▶
2018 2019 2020

11 captures
21 Jan 2016 - 29 Nov 2019

ⓘ ? ✕
f t
▼ About this capture

requiring disclosure of information without delay, an authorized law enforcement official may submit a request through compliance@uphold.com. We will not review or respond to messages sent to this email address by non-law enforcement officials. Members aware of emergency situations should contact their local law enforcement officials.

6. CHILD SAFETY MATTERS

We report all apparent instances of child exploitation we become aware of to the National Center for Missing and Exploited Children (NCMEC), including information drawn to our attention by law enforcement requests. NCMEC coordinates with the International Center for Missing and Exploited Children and law enforcement authorities around the world. If a request relates to a child exploitation or safety matter, please specify those circumstances (and include relevant NCMEC report identifiers) in any request to ensure that we are able to address these matters expeditiously and effectively.

7. DATA RETENTION AND AVAILABILITY

We will search for and disclose data that is specified with particularity in an appropriate form of legal process that we are reasonably able to locate and retrieve. We generally do not retain data for law enforcement purposes unless we receive a valid preservation request. Our [Privacy and Data Policy](#) and [Membership Agreement](#) contain information about what information may be available.

8. REQUEST FORMAT AND SCOPE

Overly broad or vague requests for information cannot be processed. At a minimum, we need the process to specifically identify the requested records with particularity and include information that allows us to identify the member account(s) at issue by user name or email address.

9. MEMBER CONSENT

If law enforcement is requesting information about a member who has provided consent to access or obtain the account information, the member should be directed to obtain that information on their own from their account.

10. MEMBER NOTIFICATION AND LEGAL PROCESS

Uphold is founded on the principle of complete transparency. Our policy is to notify people who use our service of requests for information relating to them prior to disclosure unless we are prohibited by law from doing so or in exceptional circumstances, such as in child exploitation

prohibited by law from doing so. Law enforcement officials who believe that notification would jeopardize an investigation should obtain an appropriate court order or other appropriate process establishing that notice is prohibited. If your data request draws attention to abuse of our Service, we will take action to prevent further abuse, including actions that may indicate to the member that we are aware of potential misconduct.

11. TESTIMONY

We do not provide expert testimony support. And, our records are self-authenticating pursuant to United States law and should not require testimony of a records custodian for admission. If a special form of certification is required, please include it with your process.

12. COST REIMBURSEMENT

We may seek reimbursement for costs in responding to requests for information as provided by law. Any fees will apply on a per-account basis. We may also charge additional fees for costs incurred in responding to requests.

13. SUBMISSION OF PROCESS

Our United States mailing address is: Uphold HQ, Inc. c/o CSC, 1703 Laurel Street Columbia, SC 29201. We will accept courtesy copies of process issued by law enforcement at compliance@uphold.com. Uphold will only respond to Law enforcement requests from authorized law enforcement officials who provide the information set in Section 1.

14. SPECIAL NOTES

Acceptance of legal process by any means other than personal service is for convenience only and we reserve all rights and objections, including, without limitation lack of proper jurisdiction or invalid service.



Department of the Treasury
Internal Revenue Service
3651 S IH-35
Mail Stop: 4308 AUSC
Austin, TX 78741

Date:
8/9/19
Taxpayer ID number:
570-90-5961
Hotline telephone number:
737-800-7990
Tax form:
Form 1040

8188 PJA
JAMES HARPER
618 MARYLAND AVE NE
WASHINGTON, DC 20002-5812

Reporting Virtual Currency Transactions

Dear James Harper:

Why we're writing to you

We have information that you have or had one or more accounts containing virtual currency but may not have properly reported your transactions involving virtual currency, which include cryptocurrency and non-crypto virtual currencies.

What you need to do

After reviewing the information below, if you believe you didn't accurately report your virtual currency transactions on a federal income tax return, you should file amended returns or delinquent returns if you didn't file a return for one or more taxable years. If you do not accurately report your virtual currency transactions, you may be subject to future civil and criminal enforcement activity. For more information, visit www.irs.gov/filing.

When filing amended or delinquent returns, write "Letter 6174-A" at the top of the first page of the return. Mail the original amended or delinquent return to:

Internal Revenue Service
2970 Market Street
Philadelphia, PA 19104

Reporting virtual currency transactions

Virtual currency is considered property for federal income tax purposes. Generally, U.S. taxpayers must report all sales, exchanges, and other dispositions of virtual currency. An exchange of a virtual currency (such as Bitcoin, Ether, etc.) includes the use of the virtual currency to pay for goods, services, or other property, including another virtual currency such as exchanging Bitcoin for Ether. This obligation applies regardless of whether the account is held in the U.S. or abroad. More information can be found on www.irs.gov and in Notice 2014-21 found at www.irs.gov/pub/irs-drop/n-14-21.pdf, which describes how general tax principles for property transactions apply to transactions using virtual currency.

You must report virtual currency transactions on your return, regardless of whether you received a payee statement for the transaction (such as a Form W-2, Form 1099, etc.).

Common schedules for reporting virtual currency transactions include the following:

Schedule C

If you were an independent contractor and received payment in virtual currency, you must report it in gross income for the amount of the virtual currency's fair market value, measured in U.S. dollars, as of the date and time you received the virtual currency. Gross income derived by an individual from a trade or business, carried on by the individual as other than an employee, is reported on Schedule C. This constitutes self-employment income and is subject to the self-employment tax.

For more information, you can refer to the instructions for Schedule C.

Schedule D

If you sold, exchanged, or disposed of virtual currency (e.g. Bitcoin, Ether), or used it to pay for goods or services, you have engaged in a reportable transaction and may have a tax liability. These transactions may be reportable on Schedule D. On the tax return, report the virtual currency received at its fair market value, measured in U.S. dollars, as of the date and time of the transaction.

You should maintain and review all transaction records, including bank, wallet, and exchange reports and statements to determine your basis, amount received, and other information needed for reporting on Schedule D.

For more information, you can refer to the instructions for Schedule D.

Schedule E

If you received supplemental income in the form of virtual currency, including income from rental real estate, royalties, partnerships, S corporations, estates, trusts, and residual interests in REMICs, you may need to report this on Schedule E. On the tax return, report the virtual currency received at its fair market value, measured in U.S. dollars, as of the date and time of the transaction.

You may also need to file supplemental forms (e.g. Form 8582, Passive Activity Loss Limitations). See the instructions for Schedule E for any other circumstances that may apply.

For more information, you can refer to the instructions for Schedule E.

Additional Resources

- Publication 17, Your Federal Income Tax (For Individuals)
- Instructions for Form 1040, U.S. Individual Income Tax Return
- Instructions for Form 8949, Sales and Other Dispositions of Capital Assets
- Instructions for Form 1041, U.S. Income Tax Return for Estates and Trusts
- Instructions for Form 1120, U.S. Corporation Income Tax Return

- Instructions for Form 1120-S, U.S. Income Tax Return for an S Corporation
- Instructions for Form 1065, U.S. Return of Partnership Income

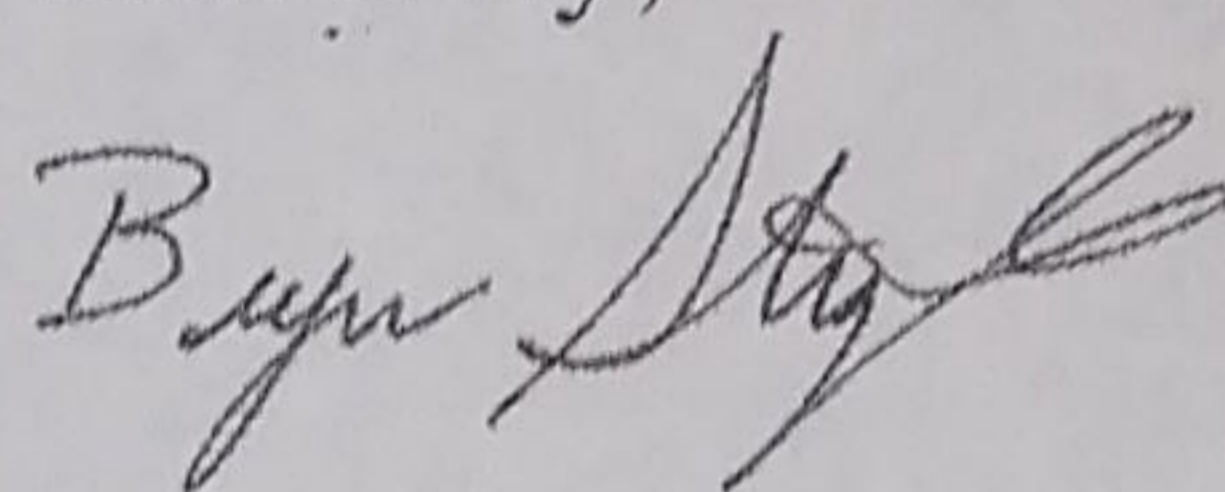
You can get the forms, instructions, and publications mentioned in this letter by visiting our website at www.irs.gov/forms-pubs or by calling 800-TAX-FORM (800-829-3676).

You do not need to respond to this letter. Note, however, we may send other correspondence about potential enforcement activity in the future.

If you have questions, you can call the hotline telephone number shown at the top of this letter and leave a message. We'll respond to all messages within three business days.

Thank you for your cooperation.

Sincerely,



Bryan Stiernagle
Program Manager



HELP

[Home](#) / [News](#) / [News Releases](#)

/ IRS has begun sending letters to virtual currency owners advising them to pay back taxes, file amended returns; part of agency's larger efforts

IRS has begun sending letters to virtual currency owners advising them to pay back taxes, file amended returns; part of agency's larger efforts

More In News

IR-2019-132, July 26, 2019

WASHINGTON — The Internal Revenue Service has begun sending letters to taxpayers with virtual currency transactions that potentially failed to report income and pay the resulting tax from virtual currency transactions or did not report their transactions properly.

"Taxpayers should take these letters very seriously by reviewing their tax filings and when appropriate, amend past returns and pay back taxes, interest and penalties," said IRS Commissioner Chuck Rettig. "The IRS is expanding our efforts involving virtual currency, including increased use of data analytics. We are focused on enforcing the law and helping taxpayers fully understand and meet their obligations."

The IRS started sending the educational letters to taxpayers last week. By the end of August, more than 10,000 taxpayers will receive these letters. The names of these taxpayers were obtained through various ongoing IRS compliance efforts.

For taxpayers receiving an educational letter, there are three variations: Letter 6173, Letter 6174 or Letter 6174-A, all three versions strive to help taxpayers understand their tax and filing obligations and how to correct past errors.

Taxpayers are pointed to appropriate information on IRS.gov, including which forms and schedules to use and where to send them.

Last year the IRS announced a [Virtual Currency Compliance campaign](#) to address tax noncompliance related to the use of virtual currency through outreach and examinations of taxpayers. The IRS will remain actively engaged in addressing non-compliance related to virtual currency transactions through a variety of efforts, ranging from taxpayer education to audits to criminal investigations.

Virtual currency is an ongoing focus area for IRS Criminal Investigation.

IRS [Notice 2014-21 \(PDF\)](#) states that virtual currency is property for federal tax purposes and provides

guidance on how general federal tax principles apply to virtual currency transactions. Compliance efforts follow these general tax principles. The IRS will continue to consider and solicit taxpayer and practitioner feedback in education efforts and future guidance.

The IRS anticipates issuing additional legal guidance in this area in the near future.

Taxpayers who do not properly report the income tax consequences of virtual currency transactions are, when appropriate, liable for tax, penalties and interest. In some cases, taxpayers could be subject to criminal prosecution.

Additional Information:

- [Virtual Currencies](#)
- [Letter 6173 \(PDF\)](#)
- [Letter 6174 \(PDF\)](#)
- [Letter 6174-A \(PDF\)](#)

Page Last Reviewed or Updated: 05-Jun-2020



Print



Our Agency

Know Your Rights

Resolve an Issue

Other Languages

Related Sites

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW HAMPSHIRE

-----X		
JAMES HARPER		CIVIL ACTION NO.: 1:20-cv-00771
	Plaintiff,	:
		:
	v.	:
		:
CHARLES P. RETTIG,		:
IN HIS OFFICIAL CAPACITY AS		:
COMMISSIONER		:
INTERNAL REVENUE SERVICE, et al.		:
		:
	Defendants.	:
-----X		

AFFIDAVIT OF MARK G. ANDERSON OF UPHOLD HQ INC.

STATE OF NEW YORK)
) ss.:
COUNTY OF NEW YORK)

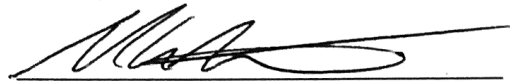
Mark G. Anderson, being duly sworn, deposes and says under penalty of perjury:

1. I am Secretary and Head of Legal and Regulatory Affairs for Uphold HQ Inc. (“Uphold”), a South Carolina corporation that is the owner and operator of the website located at www.uphold.com, and I am over 18 years of age, of sound mind and otherwise competent to make this Affidavit. The evidence set out in the foregoing Affidavit is based upon my personal knowledge.

2. I submit this Affidavit in support of the complaint filed by the Plaintiff identified above in Civil Action No. 1:20-cv-00771 in the United States District Court for the District of New Hampshire.

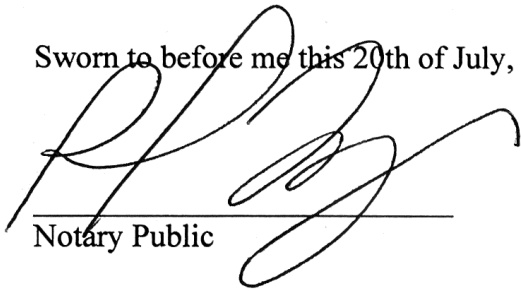
3. Uphold has conducted a thorough search of its records and has found no record of any request by the Defendants in the above-named action to produce information relating to the Plaintiff.

4. Uphold has conducted a thorough search of its records and has found no record of any information relating to the Plaintiff having been directly disclosed to the Defendants.



Mark G. Anderson
Secretary and Head of Legal & Regulatory Affairs
Uphold HQ Inc.

Sworn to before me this 20th of July, 2020:



Notary Public

PAUL FAY
Notary Public, State of New York
No. 01FA6126912
Qualified in Westchester County.
Commission Expires May 16, 2021

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW HAMPSHIRE

JAMES HARPER	:	
	:	CIVIL ACTION NO.: 1-20-cv-00771
	:	
Plaintiff,	:	COMPLAINT
	:	
v.	:	JURY TRIAL DEMANDED
	:	
CHARLES P. RETTIG,	:	
IN HIS OFFICIAL CAPACITY AS	:	
COMMISSIONER	:	
INTERNAL REVENUE SERVICE,	:	
	:	
&	:	
	:	
INTERNAL REVENUE SERVICE,	:	
	:	
&	:	
	:	
JOHN DOE IRS AGENTS 1-10,	:	
	:	
	:	
Defendants.	:	

NOTICE OF FILING AMENDED COMPLAINT UNDER FED. R. CIV. P. 15(a)(1)(A)

Plaintiff hereby gives notice of filing an Amended Complaint under Fed. R. Civ. P. 15(a)(1)(A) “as a matter of course within ... 21 days after servi[ce]” of the Complaint (ECF No. 1). Under Rule 15(a)(1), it is not necessary for the Plaintiff to secure opposing party’s written consent or the Court’s leave to file an amended complaint once as a matter of course. The District of New Hampshire Local Rule 15.1 also does not require the Plaintiff to file a motion for leave to file an amended complaint pursuant to Fed. R. Civ. P. 15(a)(1)(A).

Plaintiff filed the Complaint (ECF No. 1) on July 15, 2020. This notice, the accompanying Amended Complaint, and exhibits attached thereto, are filed and served within 21 days of serving the original Complaint. Plaintiff has filed no other amended complaint in this

case. The Defendants have not filed any responsive pleading or a motion to dismiss to render Fed. R. Civ. P. 15(a)(1)(A) inapposite in this case.

The Amended Complaint complies with Local Rule 15.1(b) because it “reproduce[s] the entire filing as amended and [does] not incorporate any prior filing by reference.”

August 5, 2020

Respectfully submitted.

Jared Bedrick

Douglas, Leonard & Garvey, P.C.
14 South Street
Concord, NH 03301
N.H. Bar No. 20438
(603)224-1988
jbedrick@nhlawoffice.com

Caleb Kruckenberg*

Litigation Counsel

Aditya Dynar*

Litigation Counsel

New Civil Liberties Alliance
1225 19th St. NW, Suite 450
Washington, DC 20036
(202) 869-5230

caleb.kruckenberg@ncla.legal

adi.dynar@ncla.legal

*Applications for Admission *Pro Hac Vice* to be filed