UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF GEORGIA

HUGO SOARES,

Civil Action No. Plaintiff,

v.

Jury Trial Demanded BITPAY, INC.,
a Delaware corporation,
Defendant.

COMPLAINT

Plaintiff Hugo Soares alleges against Defendant BitPay, Inc. ("BitPay" or the "Company") as follows:

SUMMARY

1. Founded in 2011, BitPay is a payment processor that specializes in enabling individuals and businesses to accept payments in Bitcoin and other cryptocurrencies.

2. In addition to payment services, for a time BitPay provided development, support, and maintenance services to its own open source, software based wallet for storing cryptocurrencies, which it branded "Copay" ("Copay" or the "Software"). During the relevant period, BitPay used Copay to advertise to potential customers inside the application, often touting Copay's alleged "security" and "trust" benefits, and to grow its business by cross-promoting its suite of payment services.

3. Mr. Soares began using the Copay wallet for the first time after having downloaded it from the Apple App Store in December 2017. Lacking any particular technical skill in assessing the respective merits of cryptocurrency wallets, Mr.

Soares selected Copay because it was

commonly in use in his native Brazil and he believed it to be safe.

4. Mr. Soares downloaded Copay and began using it without first being shown, reviewing, or being asked, let alone required, to consent to any terms or conditions governing Copay's use. Although Mr. Soares is now aware that the Company has since updated its policies and user agreements various times, prior to 2023, he had never personally seen the documents purportedly governing his legal relationship with BitPay.

5. On November 26, 2018, BitPay learned that malicious code had been loaded into Copay through a "supply-chain" attack in which a malicious actor was able to gain legitimate access to a widely-shared JavaScript library known as "event stream."

6. Due event-stream's popularity among developers, the malicious code was downloaded millions of times as part of other, unrelated applications. Yet, the true purpose of the malicious code was to steal Bitcoin from the narrow subset of event-stream users who happened to be running event-stream, Copay, *and* who had balances of more than 100 Bitcoin. The coincidence of these variables in exploited versions of Copay caused these wallets' corresponding private keys to be exposed and then sent off to a web address specified by the hacker.

7. Although BitPay publicized the existence and nature of the exploit on its website on December 12, 2018, and soon issued a patched version of Copay, it does not appear to have taken any additional steps to warn the public about the affected versions. In particular, it made no mention of the unique danger posed to users having balances in excess of 100 Bitcoin.

8. Similarly, the Company did not issue any warnings in Mr. Soares' native language of Portuguese or, for that matter, any other languages besides English despite having users all over the world.

9. In its December 12, 2018 post, BitPay referenced various "long-term improvements" it had made to Copay in response to the exploit, namely, by "reducing dependency risk" and "locking down network connections." In other words, the exploit was enabled by BitPay's failure to properly screen Copay's JavaScript dependencies and by its failure to place any limitations on Copay's ability to interact with any random website on the internet.

10. Had Copay not suffered from these obvious security vulnerabilities, which BitPay knew about in advance but failed to remedy, the wallet could not have been exploited in this fashion.

11. Due in part to the lack of Portuguese-language press releases or other media pertaining to the exploit, Mr. Soares unfortunately did not learn about the hack until it happened to him almost exactly one year later on November 22, 2019.

12. Mr. Soares was uniquely affected by the exploit because he happened to have a Copay wallet balance in excess of 100 Bitcoin. This threshold amount was never mentioned in any BitPay releases or communiques.

13. As a direct and proximate result of BitPay's failure to exercise ordinary care in the maintenance and development of Copay, as well as its failure to communicate actionable information to its users like Mr. Soares so that they could protect themselves from an obvious harm, Mr. Soares lost 336.2008 Bitcoin in the exploit.

14. Today, Mr. Soares' lost Bitcoin are valued at approximately $11.7 million.

NATURE OF THE PROCEEDING AND RELIEF SOUGHT 15. Mr. Soares seeks a judgment against BitPay, Inc. for negligence to compensate him for the harms he has suffered due to their acts and omissions.

JURISDICTION AND VENUE

16. This Court has jurisdiction over this action pursuant to 28 U.S.C. § 1332 because the amount in controversy exceeds $75,000 and diversity of citizenship exists among the parties. This Court likewise has jurisdiction pursuant to 28 U.S.C. § 1332(c)(1) because, at all times relevant to this Complaint, the Company's principal place of business was in Alpharetta, GA.

17. Venue is proper in this district pursuant to 28 U.S.C. § 1391 in that a substantial part of the events or omissions giving rise to the claims occurred herein.

PARTIES

18. Plaintiff Hugo Soares is an adult male and a citizen and resident of Sao Paolo, Brazil.

19. Defendant BitPay, Inc. is a Delaware corporation which maintains its headquarters at 8000 Avalon Boulevard, Suite 300, Alpharetta, GA 30009. BitPay's registered agent for service of process is Corporation Service Company located at 2 Sun Court, Suite 400, Peachtree Corners, GA 30092. At all times relevant to this Complaint, BitPay conducted business in this judicial district.

FACTUAL ALLEGATIONS

I. Defendant BitPay did not request or require Mr. Soares' consent to any agreement setting forth each party's rights and responsibilities prior to allowing him to use Copay.

20. Mr. Soares learned about Copay as he continued to buy and sell cryptocurrencies throughout 2017.

21. In December 2017, Mr. Soares had heard favorable reviews from friends and colleagues in Brazil about Copay, so he downloaded it from the Apple App Store and began using it to custody Bitcoin on his iPhone.

22. When Mr. Soares downloaded Copay from the App Store, he was not required to separately create any kind of account with BitPay, provide his personal information to BitPay, nor register his copy of the Software with BitPay.

23. At no time did the Software prompt Mr. Soares to click a box indicating "I Agree" to any particular Company policy before allowing him to use it. 24. Similarly, Mr. Soares never observed any hyperlinks in the App Store or in the Software itself referencing any Company policies. If hyperlinks did appear in the App Store or in the Software itself, they were situated among other text without any distinguishing highlighting or notations.

25. At all relevant times, Mr. Soares was unaware of any written contractual provisions governing his use of the Software.

26. Mr. Soares believed that he was free to use the Software so long as his use was not for any illegal purpose. In like fashion, Mr. Soares believed that BitPay was under an obligation to provide a functioning wallet that was secure.

27. Although a user agreement document was visible on BitPay's website around the time Mr. Soares downloaded, installed, and began using the Software, the placement of this document was also not conspicuous because it was on the website, rather than being linked directly from the Software itself, and it only appeared behind a link entitled "Terms of Use" at the bottom of the page.

28. The "Wallet Terms of Use" document that purports to have been updated on November 30, 2017 contains a total of 780 words.

29. The Wallet Terms of Use have been updated and amended at various times throughout the relevant period, but Mr. Soares has never affirmatively consented to any version of them.

30. Upon information and belief, there were instances in December 2017 when the Wallet Terms of Use did not reliably appear on the BitPay website.

31. In the middle of the Wallet Terms of Use, there is a disclaimer in non boldfaced capital letters which purports to sharply limit BitPay's liability for any harms arising out of any use of the Software.

32. Even if Mr. Soares had come across the Wallet Terms of Use, he would not have perceived it as a formal contract governing his use of the Software because he was not given an overt opportunity to review it, or even made aware of its existence, prior to installing and using the Software.

33. Upon information and belief, no technical impediment prevented BitPay from requiring users like Mr. Soares to click "I Agree" to any Company policies prior to granting them access to the Software.

34. Upon information and belief, BitPay used its own business judgment to determine that a "clickwrap" agreement was not desirable prior to granting users access to Copay.

35. Upon information and belief, BitPay opted for what might instead be considered *arguendo* a "browsewrap" agreement, despite not taking steps to ensure that the existence of the Wallet Terms of Use was reasonably conspicuous to the average user.

36. Mr. Soares cannot be bound by the Wallet Terms of Use because he was never placed on actual or inquiry notice of the agreement's existence. 37. Moreover, Mr. Soares cannot be bound by the Wallet Terms of Use because the latter constitutes inconspicuous contractual provisions of which he was not aware, and such provisions were contained in a document whose contractual nature was not obvious.

II. Defendant BitPay's failure to exercise ordinary care in managing the Software, which ultimately led to the supply chain attack, was further compounded by its failure to meaningfully communicate

news of the exploit to affected users such as Mr. Soares who had Copay wallet balances in excess of 100 Bitcoin.

a. The Nature and Genesis of the Exploit

38. In 2015, a user named "dominictarr," the creator of the event-stream package, stated that he would no longer maintain its corresponding GitHub repository.

39. On October 16, 2015, event-stream went into "maintenance mode," meaning that only minor issues were being fixed and new releases were less frequent.

40. User dominictarr's last contribution to the event-stream codebase occurred in October 2017. After this point, upon information and belief, the event stream package was not being actively maintained by its founder despite being used by a wide array of applications, including Copay.

41. Using dependencies such as event-stream is a common practice in the development of cryptocurrency wallet applications. Modern open-source application design relies on the usage of specific components that are developed and made available by others.

42. Modern software is typically written in JavaScript and then compiled for the relevant platforms. This way, applications can be written to run as standalone software on a PC or Mac, in a web environment, or as a mobile application.

43. Node Package Manager (NPM) is an open-source project manager and event-stream host. The company behind NPM is known as npm, Inc., which was founded in 2014 and acquired by GitHub in 2020.

44. NPM performs various core functions in the JavaScript world: it is the package manager created to assist JavaScript developers with easily sharing packaged modules of code; it is a command line client that allows developers to install and publish these packages; and, the NPM Registry is a public collection of

open-source JavaScript code packages for a variety of use cases, such as front-end web apps, mobile apps, routers, etc.

45. On August 5, 2018 a package called "flatmap-stream" was published on NPM by user "Antonio Macias" that seemed to offer flatmap functionality, *i.e.*, the ability to "flatten" or merge multiple collections or arrays into one. Also, during this month another dependency of flatmap-stream was published to NPM. This package did not contain any malicious code and was introduced to event-stream version 3.3.6.

46. On September 4, 2018 user dominictarr gave the user @right9ctrl (whose account has since been deleted) maintainer access to the event-stream GitHub repository and transferred publishing access on NPM for event-stream.

47. Event-stream version 3.3.6 was released on September 9, 2018. 48. Then, on October 5, 2018, flatmap-stream version 0.1.1 was released, having been infected with malicious code.

49. All products using event-stream 3.3.6 upgraded to the infected version of flatmap-stream during the build process for each new version. The hacker introduced this malicious version making it appear as though it were a minor update.

50. The malicious code was deployed in two stages. The first stage occurred during the build of the project, while in the second, malicious code was written into the application.

51. During the first stage, the malicious code detected whether the dependency was running in the target package. If so, it was transformed into valid JavaScript which could then be added to the infected application–*i.e.*, Copay versions 5.0.2 to 5.1.0–waiting to be shipped out to users' devices.

52. In the second stage, the malicious code was executed by the infected application, first checking whether the application was Copay for desktop, iOS, or Android. Then, the malicious code located certain user account data, ***checked for a***

balance of 100 Bitcoin or more, and

proceeded to send the infected user's private keys to a server which the hacker controlled.

53. In possession of the private keys, the hacker could then transfer the funds to any wallet of their choosing.

b. BitPay's Response

54. On November 26, 2018, BitPay released a statement on its blog advising users to not open the Copay application, but to instead transfer funds from affected wallets to new wallets using a safe version of the Software.

55. Once news of the exploit became public, an "issue" was opened in the Copay GitHub repository notifying Copay developers of the discussion occurring in the event-stream repository.

56. On November 27, 2018 Copay developer @matiu described in the GitHub thread the steps that were being taken to improve the Software:

> "We will be taking multiple measures to mitigate future issues like this one. The dependencies problem on node.js is a huge problem and many projects are facing issues like this. Almost 4000 projects were "infected" just to access Copay. On the other hand, trying to build a competitive app, GUI-wise, multiplatform not using JS seems impossible.
>
> Some of the measures we are doing:
>
> 1. Freeze dependencies and add them to the repo, so we can see diff when upgrading deps. This will be practical sometimes, be [sic] definitely not always.
> 2. Restrict network access within the app.
> 3. Create a new app, with very few dependencies, to sign TXs. This is already working in our CLI app and air-gapped signer.
> 4. Freeze critical classes to prevent function over-write.
> 5. Refactor storage, to only allow access from certain code parts."

57. On December 12, 2018 BitPay released a follow-up statement detailing measures it had taken to shore up Copay's security, which included greater due diligence in dependency verification and whitelisting URLs for network connections.

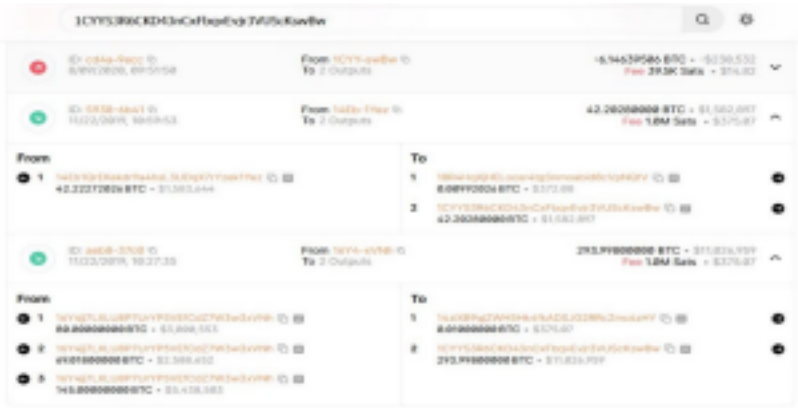
58. In particular, the Company said that reducing its dependency risk by only updating dependencies when a major version of Copay is released "makes it easier to review dependencies in our codebase before those changes go live for our users." This practice of "pinning" dependencies was a common security measure in the JavaScript industry well prior to the Copay exploit.

59. With regard to network connections, the Company said, "By restricting the URLs that the Copay […] app […] can interact with, we make it harder for this kind of attack to work even if an attacker found their way into our codebase."

60. Upon information and belief, the Company never conducted, or mandated that a third-party conduct, an audit of the Copay application. 61. Having at least one audit performed by a reputable organization was also standard industry practice at the time for applications involving user funds. 62. Although articles regarding the exploit would sometimes appear in third-party technology publications for a short time thereafter, upon information and belief, the Company did not conduct any additional, targeted effort to notify affected users worldwide other than what is described generally in this Complaint. **c. Mr. Soares' 336.2008 Bitcoin**

63. Mr. Soares' Bitcoin addresses corresponding to his Copay wallet are 16Y4jj7LXLU8P7UrYP5VEfCdZ7W3w3xVNh and 14Eb1QrEKekdr9a4hsL3U DqX7rYzek1Yez. The hacker's wallet which received the funds is 1CYYS3R6CKD43nCxFbqvEvj r3VUScKswBw.

64. The immutable record on the Bitcoin blockchain shows the transfer of 336.2008 Bitcoin from wallets controlled by Mr. Soares to those of the hacker occurring on November 22, 2019:



65. On November 27, 2019 Mr. Soares posted the following panicked message on the bitcointalk.org message board:

> "I've experienced what it seems [sic] a huge exploit in my copay wallet, with 336.2008 btcs beeing [sic] moved out. This is a new phone use only [sic] for btc, never in public wifi, never downloaded anything other than essencial [sic] apple apps, etc.
>
> All of the sudden [sic] 3 withdraws from otc dealers were confirmed my wallet sent 293.998 btcs to the address(below), [sic] i thought was a normal wallet re-sync(as it happens almost weekly in copay where u dont [sic] see your funds) After receiving my balance, my wallet again sent it to the address.
>
> Tried already restoring in other wallets and in others deviaton [sic] path, no success, looks like a hacking/exploit situation.
>
> Help!!"

66. The Company was on notice that its userbase spanned many countries, yet it took no steps to notify users, such as Mr. Soares in Brazil, that his Bitcoin were in jeopardy.

67. Had the Company taken any remedial action whatsoever directed at users like Mr. Soares, Mr. Soares' losses could have been prevented. 68. Upon information and belief, BitPay took no additional remedial measures directed at potentially vulnerable users after December 12, 2018. 69. Rather, BitPay appears to have deleted its blog post regarding the exploit at some point shortly thereafter.

FIRST CLAIM FOR RELIEF

Negligence

70. Mr. Soares realleges and incorporates by reference the preceding and successive paragraphs as though fully set forth herein.

71. Defendant BitPay, Inc. had a duty to exercise the same level of care in all matters concerning Copay that a reasonable person would have exercised under the same circumstances.

72. Defendant BitPay, Inc. breached its duty of ordinary care to Mr. Soares in a manner including, but not necessarily limited to, the following: a. Failing to review dependencies in advance of their incorporation to the Software;

b. Failing to test new releases for suspicious behavior or securing the build environment used for new releases;

c. Failing to restrict the introduction of updates to only those subject to prior manual vetting;

d. Failing to restrict network access within the Software to only whitelisted addresses;

e. Failing to perform, or have a third-party perform, a security audit of the Copay wallet;

f. Failing to meaningfully warn users such as Mr. Soares of the exploit;

g. Failing to sufficiently mitigate harm to users such as Mr. Soares; h. Failing to disclose or meaningfully publicize the peculiar detail that the exploit only affected Copay wallets having a balance greater than 100 Bitcoin, such as Mr. Soares'.

73. Defendant BitPay, Inc.'s breaches of its duty were the but-for and proximate causes of Mr. Soares' losses.

PRAYER FOR RELIEF

WHEREFORE, Mr. Soares respectfully requests that this Court enter Judgment:

1. Finding that Defendant BitPay, Inc. committed the violations set forth in this Complaint;

2. Ordering that Defendant BitPay, Inc. pay damages, costs, and other expenses arising as a consequence of its aforementioned violations of law; and 3. Granting such other and further relief as the Court deems just and proper.

JURY TRIAL DEMAND

Pursuant to Rule 38 of the Federal Rules of Civil Procedure, Plaintiff Hugo Soares demands that this case be tried to a jury.

Dated: November 16, 2023 Respectfully submitted,

INDUSTRIA BUSINESS LAWYERS LLP
601 Pennsylvania Avenue NW
S Building, Suite 900
Washington, DC 20004
admin@iblpartners.com
Tel: (202) 495-1185

By: **Matthew J. Bouillon Mascareñas**

Attorney Bar Number: 351584 Attorney for Plaintiff Hugo Soares
Tel: (404) 513-0750 Email: matthew@iblpartners.com

Livecoins.com.br