Thiago M. Coelho, SBN 324715
thiago@wilshirelawfirm.com
Carolin K. Shining, SBN 201140
cshining@wilshirelawfirm.com
Jonas P. Mann, SBN 263314
jmann@wilshirelawfirm.com
Jennifer M. Leinbach, SBN 281404
jleinbach@wilshirelawfirm.com
Jesenia A. Martinez, SBN 316969
jesenia.martinez@wilshirelawfirm.com
Jesse S. Chen, SBN 336294
jchen@wilshirelawfirm.com
WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd., 12th Floor
Los Angeles, California 90010
Telephone: (213) 381-9988
Facsimile: (213) 381-9989

Attorneys for Plaintiff and Proposed Class

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

CHARLES FREEMAN, TIGRAN MELKONYAN, ARI SHOFET, SHAWN MALL, BENJAMIN FERRIS, BRYAN CHAPMAN, NANDAN ARORA, SHAFIQ RAJANI, VIJAY CHRISTOPHER, MARC ASHBY, VINCENT VAN BUSKIRK, LAWRENCE MANICKAM, and EDMUNDO PENA individually and on behalf of all others similarly situated,

Plaintiffs,

v.

3COMMAS TECHNOLOGIES OÜ, an Estonian Private Limited Company

Defendant.

Case No.:

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Plaintiffs Charles Freeman, Tigran Melkonyan, Ari Shofet, Shawn Mall, Benjamin Ferris, Benjamin Chapman, Nandan Arora, Shafiq Rajani, Vijay Christopher, Marc Ashby, Vincent Van Buskirk, Lawrence Manickam and Edmundo Pena ("Plaintiffs"), individually and on behalf of all others similarly situated, bring this action against Defendant 3Commas Technologies OÜ ("3Commas" or "Defendant") based upon personal knowledge as to themselves and their own acts, and as to all other matters upon information and belief, based upon, *inter alia*, the investigations of their attorneys.

SUBSTANTIVE ALLEGATIONS

A. Cryptocurrency and Crypto Trading Bots

1. Cryptocurrencies, or Crypto, are digital currencies designed to work as a medium of exchange through a computer network that is not reliant on a central authority, such as a government or bank, to uphold or maintain it. Individual units of a Cryptocurrency ("Coins") are typically stored and verified in a distributed ledger or "Blockchain." Blockchains use peer-to-peer computer networks and consensus algorithms to reliably replicate the contents of the ledger across multiple computer end-points—thus ensuring that all transaction data is recorded reliably and accurately. In other words, Blockchains verify Coin transfers, as well as control the creation of additional Coins, whilst eliminating the need for traditional intermediaries—thus allowing Cryptocurrencies to serve as value-holding assets.

2. Despite their name, Cryptocurrencies are not considered currencies in the traditional sense, and are generally viewed as a distinct asset class. In recent years, Cryptocurrencies such as Bitcoin and Ethereum have exploded in value, with a single Coin commanding prices of approximately $17,157.90 and $1,270.42 respectively.

3. Defendant 3Commas is a provider of automatic Crypto trading software, or "Bots." Similar to automated stock trading systems, a Crypto trading "Bot" is a piece of software that automatically makes trades on Cryptocurrency exchange platforms when certain pre-determined conditions are satisfied. Crypto trading Bots, such as those that 3Commas offers, analyze the crypto market based on technical indicators, price levels, and volatility to decide when and whether a trade should be made. The use of such Bots is widely recognized as more efficient

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

and profitable than manual trading, and trades made by Bots make up approximately 80% of total Crypto trades.[1]

4. On its Twitter profile, 3Commas claims to provide the "largest crypto trading software" and that it processes up to $23 billion in monthly volume.[2] It has further claimed that it is "the most popular automated trading platform with the most advanced trading tools."[3] 3Commas currently offers Bots for the following Cryptocurrency exchange platforms: Crypto.com, Binance, Bittrex, Bitstamp, Bitfinex, Bitmex, Coinbase, OKX, KuCoin, Deribit, Gate.io, Gemini, Huobi, and Kraken. 3Commas offers its services in tiers "Starter," "Advanced," and "Pro" which are priced at $29/month, $49/month, and $99/month, respectively.

B. Authorizations and API Keys Required for Crytpo Trading Bots

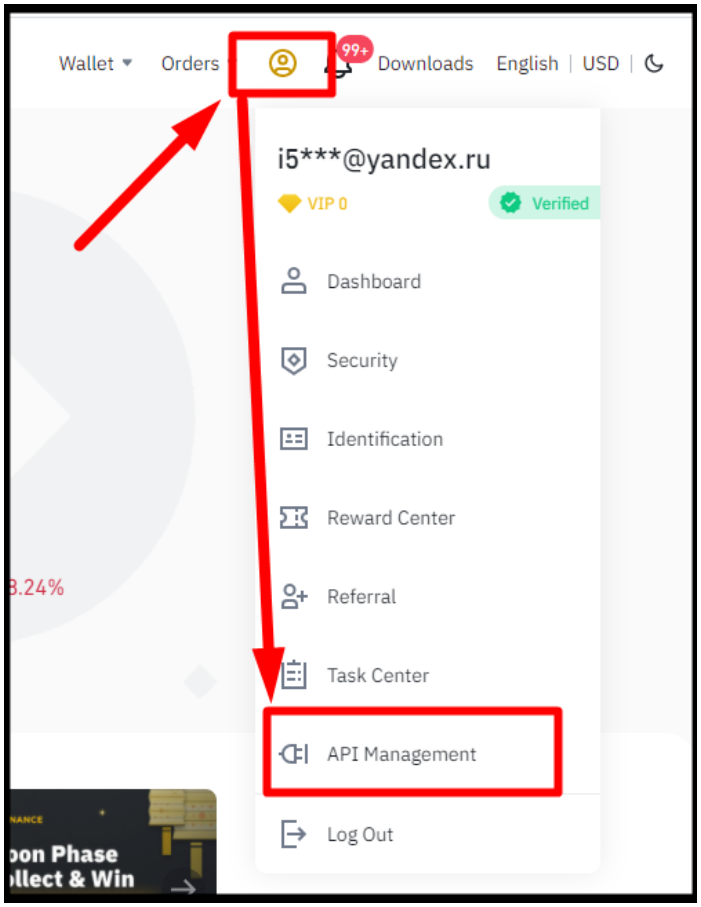
5. In order to perform automatic trades on any Cryptocurrency exchange platform, Crypto trading Bots require access to an application programing interface ("API") key—secret credentials generated by each platform which grant third parties such as 3Commas permission to trade on a user's behalf. Cryptocurrency exchange platforms use API keys for, *inter alia*, authenticating the identity and permissions of a user that makes a trade on their platform.

6. 3Commas requires each customer to provide a corresponding API key in order to use their Bots on Cryptocurrency exchange platforms. A separate API key is required for each separate Cryptocurrency exchange platform. As API keys must be manually generated on each platform by users themselves (*see, e.g., Figure 1* below), 3Commas directs its customers to generate specific API keys for each Cryptocurrency exchange platform, and to provide each specific key to 3Commas in order to use its Bots on the corresponding platform.

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

[1] "What are Crypto Trading Bots" https://3commas.io/blog/what-are-crypto-trading-bots (last accessed January 6, 2023).
[2] https://mobile.twitter.com/3commas_io/with_replies (last accessed December 13, 2022).
[3] October 19th Phishing Attack Post Mortem" https://3commas.io/blog/october-19-phishing-attack-post-mortem (last accessed December 13, 2022).

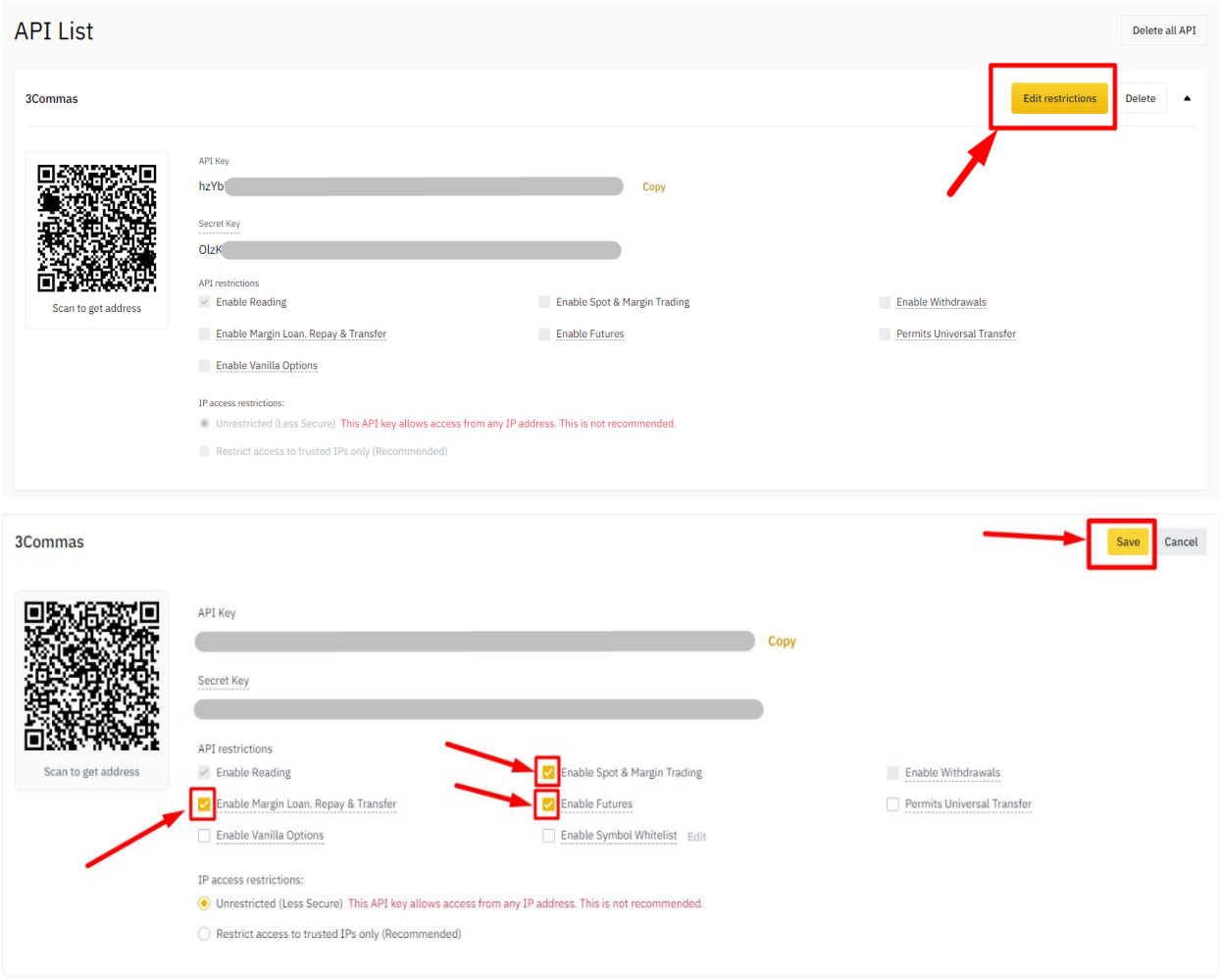
Figure 1
Example of a creation of an API Key for 3Commas on Binance



WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

7. After a user has created the API key, 3Commas then directs its customers to edit the restrictions set upon the API to grant the Bot access to certain trading functions. Specifically, 3Commas directs its customers to enable permissions for Margin Loan, Repay & Transfer, Spot & Margin Trading, and Futures. *See, e.g., Figure 2* below.

Figure 2
Enabling Permissions Required for 3Commas to Operate on Binance



C. 3Commas' API Keys Used to Compromise Customer Portfolios and Facilitate Fraudulent Trading

8. Starting in or around October of 2022, 3Commas users began noticing that their accounts on various Cyrptocurrency exchange platforms, including, *inter alia*, Binance, Coinbase, KuCoin, Bittrex, FTX and OKX, had been ransacked. A nefarious actor or actors had exploited those users' API keys and other API data to make copious unauthorized trades, costing

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

some users up to hundreds of thousands of dollars in lost value. As one victim stated: "There were dozens and dozens and dozens of trades…Basically, they used my API details to sell all of my assets into a low-cap, low-liquidity coin," resulting in a total loss of $200,000.[4]

9. Between October and November of 2022, at least forty-eight 3Commas customers were identified as victims of similar attacks.[5] Binance and Coinbase confirmed to several victims that the nefarious actor(s) responsible for the attacks had used API keys provided to 3Commas to facilitate the fraudulent trades.[6] This prompted widespread speculation that 3Commas had leaked customer APIs or otherwise had their API database exposed.

10. To combat these rumors, 3Commas published a blog post on November 1, 2022. In that blog post, 3Commas confirmed that some of its users' API keys had been stolen but claimed that here had been "no breaches on the account security and API encryption systems of 3Commas or our partner exchanges."[7] Instead, 3Commas strongly asserted that hackers had stolen the API keys from the victims individually through phishing schemes.

11. Phishing is the fraudulent practice of sending emails or other messages purporting to be from a reputable company in order to induce individuals to reveal sensitive personal information, such as passwords or financial account information, to the phisher. An example of a common phishing scheme is as follows: An email arrives claiming to be from Paypal, informing an individual that their account has been compromised and will be deactivated unless they confirm their credit card details and containing a link to do so. That link will then lead to a fake website designed to imitate the look and feel of the actual Paypal website, where the individual will be directed to enter their credit card information. The fake website will then transmit that individual's inputted credit card information to the phisher, who may then use it to commit fraud

[4] "Alameda-Backed Crypto Trading Firm 3Commas Says It's Pretty Sure It Wasn't Breached." https://www.coindesk.com/tech/2022/11/23/alameda-backed-crypto-trading-firm-3commas-says-its-pretty-sure-it-wasnt-breached/ (last accessed January 6, 2023).

[5] Response to False Rumors of API Leaks or Exposure of our Database" https://3commas.io/blog/response-to-false-rumors-api-leaks (last accessed December 13, 2022).

[6] *Id.*

[7] "October 19th Phishing Attack Post Mortem" https://3commas.io/blog/october-19-phishing-attack-post-mortem (last accessed December 13, 2022).

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

or other crimes.

12. In its November 1, 2022 blog post, 3Commas claimed that nefarious actors had created just such a "fake website resembling the automatization engines' interfaces on its own website and lured a few customers into re-entering API keys."[8] 3Commas would go on to claim that its investigation into the attacks had "identified multiple cloned websites with slight variations of the 3Commas URL."[9] Finally, 3Commas reported that the total loss resulting from these first attacks "totaled around $6M across all exchanges."[10]

13. 3Commas would maintain its unequivocal stance that the attacks were attributable solely to phishing attacks against individual customers in the face of an ever-growing list of victims. On October 23, 2022, 3Commas released the following statement:

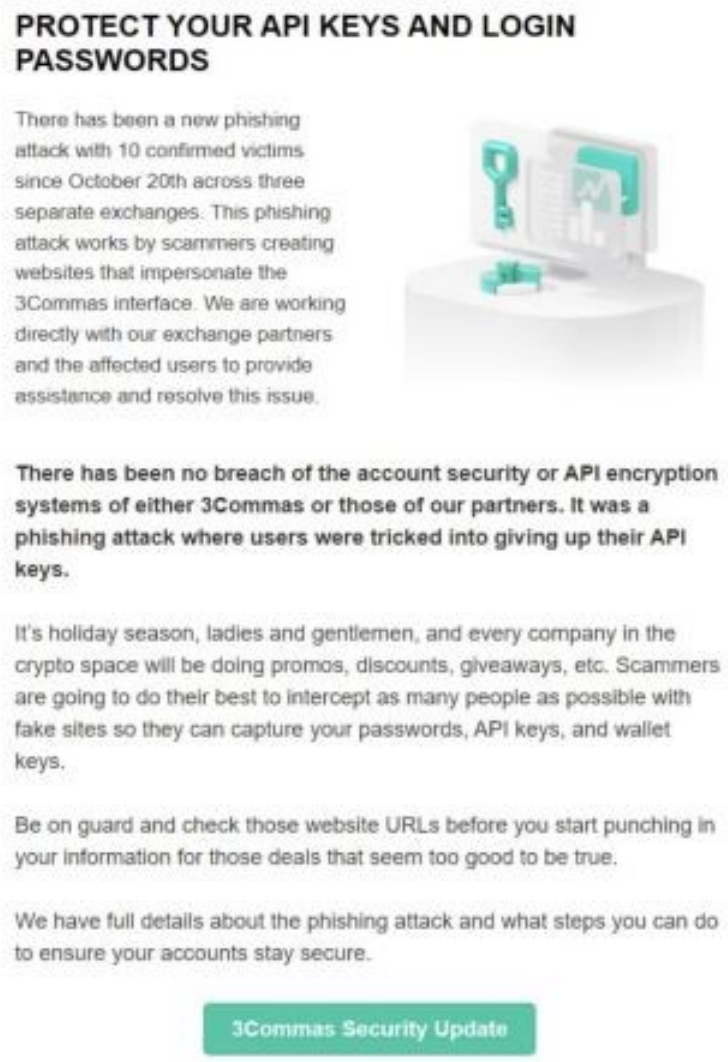
> To reiterate and clarify, **there has been no breach of either 3Commas account security databases of API keys**. This is an issue that has affected multiple users who have never been customers of 3Commas so **there is no possibility that it is a leak of API keys originating from 3Commas**.[11]
> (Emphasis added.)

14. On that same day, 3Commas also published a security alert and newsletter, which stated that: "**There has been no breach of the account security or API encryption systems of either 3Commas or those of our partners. It was a phishing attack where users were tricked into giving up their API keys**." (emphasis in original.) *See Figure 3*, below.

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

[8] *Id.*
[9] *Id.*
[10] *Id.*
[11] "3 Commas issues security alert as FTX deletes API keyes following hack" https://cointelegraph.com/news/3commas-issues-security-alert-as-ftx-deletes-api-keys-following-hack (last accessed December 13, 2022).

Figure 3
3Commas October 23, 2022 Security Newsletter



PROTECT YOUR API KEYS AND LOGIN PASSWORDS

There has been a new phishing attack with 10 confirmed victims since October 20th across three separate exchanges. This phishing attack works by scammers creating websites that impersonate the 3Commas interface. We are working directly with our exchange partners and the affected users to provide assistance and resolve this issue.

There has been no breach of the account security or API encryption systems of either 3Commas or those of our partners. It was a phishing attack where users were tricked into giving up their API keys.

It's holiday season, ladies and gentlemen, and every company in the crypto space will be doing promos, discounts, giveaways, etc. Scammers are going to do their best to intercept as many people as possible with fake sites so they can capture your passwords, API keys, and wallet keys.

Be on guard and check those website URLs before you start punching in your information for those deals that seem too good to be true.

We have full details about the phishing attack and what steps you can do to ensure your accounts stay secure.

3Commas Security Update

15. In a November 14, 2022 blog post, 3Comma's CEO Yuriy Sorokin characterized any allegations that 3Commas had leaked customer credentials as "false rumors."[12] In a November 18, 2022 tweet, 3Commas confidently stated that "[o]ver the past month, there have been multiple incidents of unauthorized trades on partner exchanges," that "[w]e've identified that these users' API keys were accessed through a variety of phishing and input-stealing methods," and that "[w]ith your help, we're fighting back against the bad actors who attacked our

[12] "Response to False Rumors of API Leaks or Exposure of our Database" https://3commas.io/blog/response-to-false-rumors-api-leaks (last accessed December 13, 2022).

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

users."[13]

16. However, many of 3Commas' affected customers, the vast majority of whom are sophisticated and experienced Crypto traders, found these explanations unconvincing at best. Several affected customers insisted that they found no 3Commas phishing websites in their browser histories.[14]

17. Further, many affected customers reported using additional security protocols to protect their API keys and secure their accounts. [15] These precautions included bookmarking the official 3Commas website and only utilizing that bookmark to visit the website or configuring two-factor authentication to secure their accounts. Two-factor authentication is an advanced user-authentication method in which a user must provide two or more pieces of evidence in order to access an account. These added security protocols could not have been breached by the phishing described in 3Comma's blog posts.

18. One affected customer reported that he connected his Binance exchange account to 3 Commas using Binance's "Fast API" service.[16] This Fast API service allows a Binance user to configure their account to "automatically generate API keys and bind to third-party link platforms, so that [they] can start using their services without manually creating API keys."[17] A customer using Binance's Fast API service would never have to manually enter their API Key into the 3Commas website. In other words, it is inconceivable that a customer using Binance's Fast API service could have their API key phished in the manner described in 3Comma's November 1, 2022 blog post. Nevertheless, this affected customer reported losing $300,000 to

[13] https://twitter.com/3commas_io/status/1593641804762677249 (last accessed December 13, 2022).
[14] "Alameda-Backed Crypto Trading Firm 3Commas Says It's Pretty Sure It Wasn't Breached." https://www.coindesk.com/tech/2022/11/23/alameda-backed-crypto-trading-firm-3commas-says-its-pretty-sure-it-wasnt-breached/ (last accessed January 6, 2023).
[15] *Id.*
[16] *Id.*
[17] "What is Fast API and How Does It Work" https://www.binance.com/en/support/faq/what-is-fast-api-and-how-does-it-work-6aa7e2253c544d91b60746bfd03fd75d (last accessed December 13, 2022).

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

the attack.[18] His final statement on the subject was as follows:

> [3Commas has] known about this for up to a month and they could have taken more decisive action," the U.K. entrepreneur told CoinDesk. "They have put out blog posts without any direct warnings, and all of the warnings are the party line that customers have been phished for their API details. **But their claim just doesn't stand up**.[19]
> (Emphasis added.)

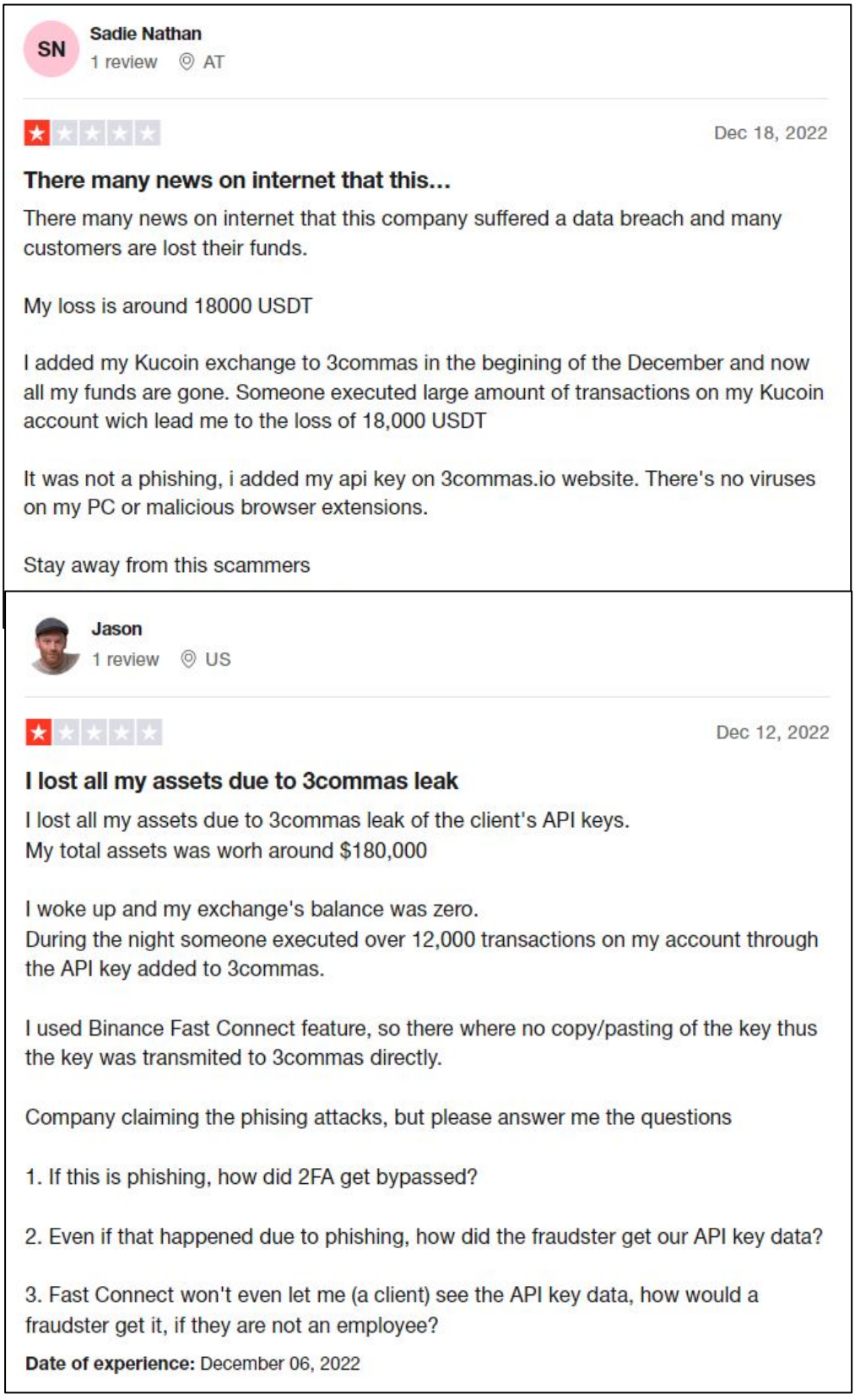
19. Indeed, 3Commas would start to walk back their unequivocal claim that every user who suffered an API attack was the victim of phishing before the end of the month. When asked about what actually caused the attacks in a November 21, 2022 interview, 3Commas Deputy Chief Technology Officer Artem Kolstov stated that "[w]e cannot be 100% sure. We definitely know that there are phishing sites out there. But also, whenever you ask the user, most of them will say…'I have never dropped my keys anywhere.'"[20] When asked about denials of phishing from users, Kolstov stated that "there's no way to check it all"[21] and that "nothing can be told for sure,"[22] confirming that 3Commas was simply not sure of that actual root cause of the attacks.

20. Attacks against 3Commas customers have continued since, with new victims surfacing at a rapid pace. Many attacks were coordinated to occur during holidays such as Thanksgiving Day and Christmas Day, when the attackers knew that the account owners were least likely to be paying attention to their Crypto accounts. Affected customers have taken to social media to demand transparency and accountability. Some affected victims have left reviews on Trustpilot, a consumer business review website, disputing 3Commas' phishing narrative and claiming tens to hundreds of thousands of dollars in losses. *See Figure 4* below.

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

[18] "Alameda-Backed Crypto Trading Firm 3Commas Says It's Pretty Sure It Wasn't Breached." https://www.coindesk.com/tech/2022/11/23/alameda-backed-crypto-trading-firm-3commas-says-its-pretty-sure-it-wasnt-breached/ (last accessed January 6, 2023).
[19] *Id.*
[20] *Id.*
[21] *Id.*
[22] "Investors claim 3Commas was breached after phishing attack" https://crypto.news/investors-claim-3commas-was-breached-after-phishing-attack/ (last accessed December 13, 2022).

Figure 4
Trustpilot Reviews



SN

Sadie Nathan
1 review AT

Dec 18, 2022

There many news on internet that this...

There many news on internet that this company suffered a data breach and many customers are lost their funds.

My loss is around 18000 USDT

I added my Kucoin exchange to 3commas in the begining of the December and now all my funds are gone. Someone executed large amount of transactions on my Kucoin account wich lead me to the loss of 18,000 USDT

It was not a phishing, i added my api key on 3commas.io website. There's no viruses on my PC or malicious browser extensions.

Stay away from this scammers

Jason
1 review US

Dec 12, 2022

I lost all my assets due to 3commas leak

I lost all my assets due to 3commas leak of the client's API keys.
My total assets was worh around $180,000

I woke up and my exchange's balance was zero.
During the night someone executed over 12,000 transactions on my account through the API key added to 3commas.

I used Binance Fast Connect feature, so there where no copy/pasting of the key thus the key was transmited to 3commas directly.

Company claiming the phising attacks, but please answer me the questions

1. If this is phishing, how did 2FA get bypassed?

2. Even if that happened due to phishing, how did the fraudster get our API key data?

3. Fast Connect won't even let me (a client) see the API key data, how would a fraudster get it, if they are not an employee?

Date of experience: December 06, 2022

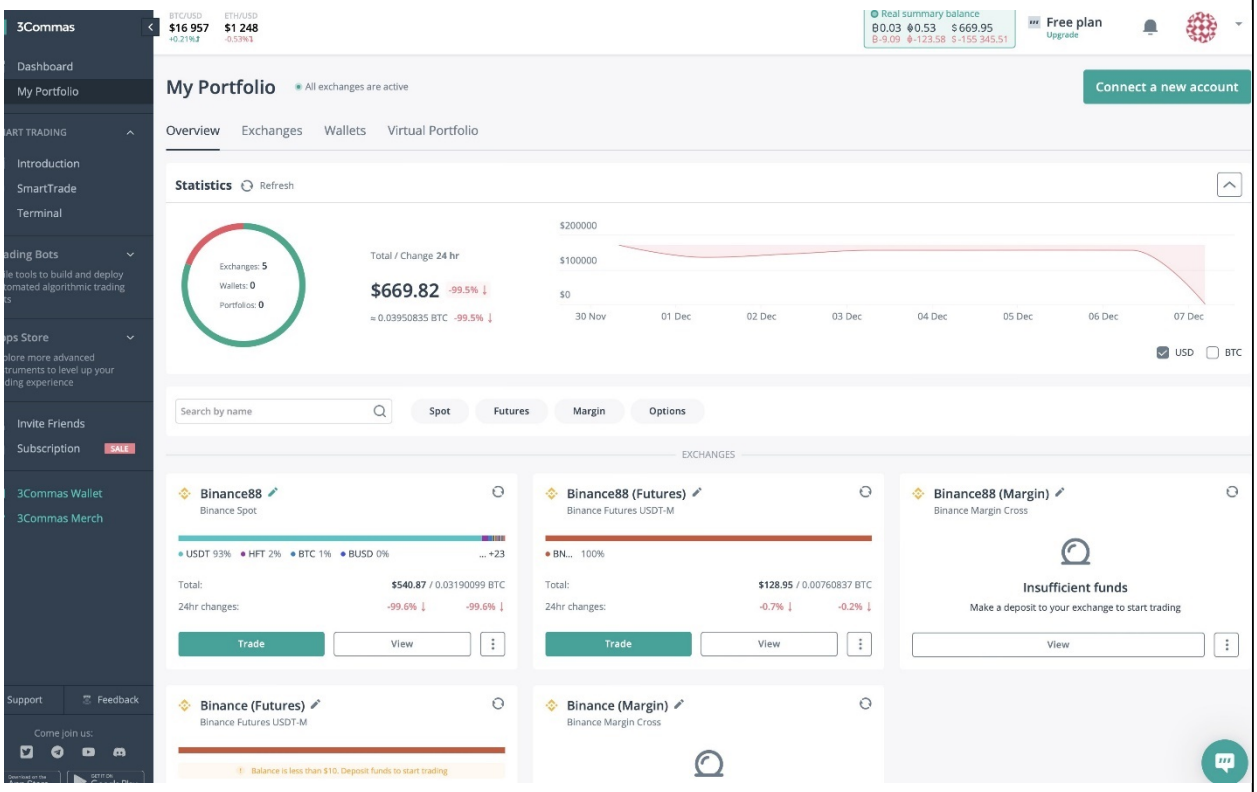
WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

21. Another victim took to Twitter, writing that:

> On 12/6/22, A 3Commas API (Free Account) I setup over 2 Years ago and forgot about suddenly became active and began performing unauthorized trades on my Binance Account:
> - $155K Losses (Contra-Traded)
> 3 Commas failed to protect customer API data. 3Commas is NOT Safe.[23]

22. This victim also included logs of the hundreds of unauthorized trades described in their tweet and a trade log summary:

Figure 5
Unauthorized API Trade Log Summary
(showing a graph of trades from November 30 - December 6, 2022)



[23] https://mobile.twitter.com/akng1985/status/1600449703728271366?cxt=HHwWjMDS-dSh-LUsAAAA (last accessed December 13, 2022).

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

23. The sheer volume of customer complaints regarding these attacks has prompted some Cryptocurrency trading platforms, such as Binance, to consider "block[ing] all 3Comma access if they don't have good ways to fix API leaks in [*sic*] their side."[24] Binance's CEO has also cautioned users to delete unused API keys and asked them to be careful when using 3Commas, noting that "[w]e seen [*sic*] at least 3 cases of users who shared their API key with 3rd party platforms (Skyrex and 3commas), and seen [*sic*] unexpected trading on their accounts."[25]

24. Regardless, 3Commas continued to lay the blame for the attacks on users themselves and phishing schemes, stating that "we have hard evidence that phishing was at least in some part a contributory factor."[26] 3Commas would stand firm on this position until the evidence that they were the source of the API leaks became undeniable.

D. 3Commas Confirms Data Breach Only after Hacker Announces Leak

25. On or around December 28, 2022, an unknown hacker revealed through a (now deleted) Pastebin post that they had gained access to the 3Commas database. With this access, they were able to steal user API keys and perform unauthorized transactions across various Crypto exchanges. To back up their claims, this hacker included a link containing several stolen API keys with their post, claiming that they would publish over 100,000 such stolen API keys "randomly in the upcoming days."[27] By way of implication via 3Commas' own previous public statements, that 'over 100,000' figure may comprise the API keys of the **entirety** of 3Commas' active userbase.[28]

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

[24] "Binance threatens to cut off 3commas access to its platform, here's why" https://ambcrypto.com/binance-threatens-to-cut-off-3commas-access-to-its-platform-heres-why/ (last accessed December 13, 2022).
[25] *Id.*
[26] "3Commas denies staff members stole API keys" https://ambcrypto.com/binance-threatens-to-cut-off-3commas-access-to-its-platform-heres-why/ (last accessed December 13, 2022).
[27] "Anonymous Twitter User Leaks 3Commas API Database" https://www.coindesk.com/tech/2022/12/28/anonymous-twitter-user-leaks-alleged-3commas-api-database/ (last accessed January 7, 2023).
[28] ""October 19th Phishing Attack Post Mortem" https://3commas.io/blog/october-19-phishing-attack-post-mortem (last accessed December 13, 2022).

26. In that same post, the unknown hacker stated that "3Commas [] sold your information to the biggest bidder and now they claim that the problem is not on their side,"[29] indicating that they had obtained the stolen API keys directly from 3Commas themselves either through illicit purchase from 3Commas or at least through a direct exploit, and not by phishing individual 3Commas users.

27. It was only after this announcement that 3Commas acknowledged that it had been breached, and that hackers had leaked user API data. On that same day, following the wide dissemination of the hacker's Pastebin post, CEO Yuriy Sorokin confirmed that the hack was genuine, stating that "[w]e saw the hacker's message and can confirm that the data in the files is true."[30] This confirmation was reiterated in a blog post made the next day.[31]

28. To date, the 3Commas leak has led to nearly $22 million in Crypto being stolen from users.[32]

29. Upon knowledge and belief, 3Commas was aware prior to the hacker's announcement that their API database had been breached and that user API keys had been leaked from their end. 3Commas was also aware that, at all times, they had not implemented adequate and reasonable data security procedures to protect their customers' PII, including sensitive API data that users are *required* to surrender in order to use 3Commas'services. Despite this, 3Commas did not take accountability for the leak, and instead deflected responsibility by passing the buck to individual users, who they claimed fell victim to avoidable phishing schemes or other hacks—despite many victims demonstrating that their API data had not and could not have been phished.

[29] https://pastebin.com/sFyhJ1xF (last accessed December 28, 2022, now deleted).

[30] https://twitter.com/YS_3Commas/status/1608202390121111552?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1608202390121111552%7Ctwgr%5E6fe6a1d33c624b7930e43b124f126b466c728540%7Ctwcon%5Es1_&ref_url=https%3A%2F%2Fwww.publish0x.com%2Fembed%2Ftwitter%2Ftweet%3Fid%3D1608202390121111552.

[31] "Notice on API data disclosure incident" https://3commas.io/blog/notice-on-api-data-disclosure-incident (last accessed January 3, 2023).

[32] "3Commas finally confirmed to be source of $22 million Hack" https://www.publish0x.com/zeroex/3commas-finally-confirmed-to-be-source-of-22-dollars-million-xozwyvv (last accessed January 3, 2023).

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

30. Worse, 3Commas staunchly maintained its evasive position in the face of months of user backlash– even posting on the same day of the Pastebin reveal that "[t]here is no API leak on 3Commas."[33] It was only when the evidence became undeniable, and their position of denial completely untenable, that 3Commas finally admitted to the breach and began taking action to revoke all breached API keys on their end.

31. Had 3Commas come forward and admitted within a reasonable time that it had suffered a data breach which leaked the API keys of, at minimum, over 100,000 of its users, 3Commas users could have and would have taken prophylactic steps sooner to protect their linked Cryptocurrency accounts. Further, 3Commas could have and should have revoked all API keys connected to their website as soon as they discovered that the API attacks could not be attributed solely to phishing schemes carried out on its users. Instead, 3Commas adamantly denied accountability for the breach, and only revoked breached API keys *after* evidence of their breach was undeniable and mass numbers of its users' API keys were publicly leaked.

E. 3Commas' Lack of Encryption for Sensitive API Data

32. Independent investigation into the 3Commas website shows that 3Commas stores and transmits sensitive API data, including API keys, API Secrets, and Passphrases in plaintext format, *without encryption*. An API Secret is generated in combination with an API key and may be used in tandem with an API key to access a user's trading accounts. A Passphrase is a secondary password that can be set by a user that may be additionally required to access a user's trading accounts.

33. Evidence that 3Commas does not encrypt API data can be found by accessing its website code on webpages where it asks you to provide sensitive information, such as API data. This can be done by visiting the "My Portfolio" webpage (*see Figures 6-8* below) and pressing the green "Connect a new Account" button on the Google Chrome browser with "Developer

[33]https://twitter.com/3commas_io/status/1608102468688265223?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1608102468688265223%7Ctwgr%5E6a5bc029102b7abb2779d79e2c8f605a705581ab%7Ctwcon%5Es1_&ref_url=https%3A%2F%2Fwww.publish0x.com%2Fembed%2Ftwitter%2Ftweet%3Fid%3D1608102468688265223.

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

Tools" open.[34] Doing so will open a pop-up window with options to connect to various Cryptocurrency exchanges.

Figure 6
3Commas My Portfolio Webpage with Developer Tools Open

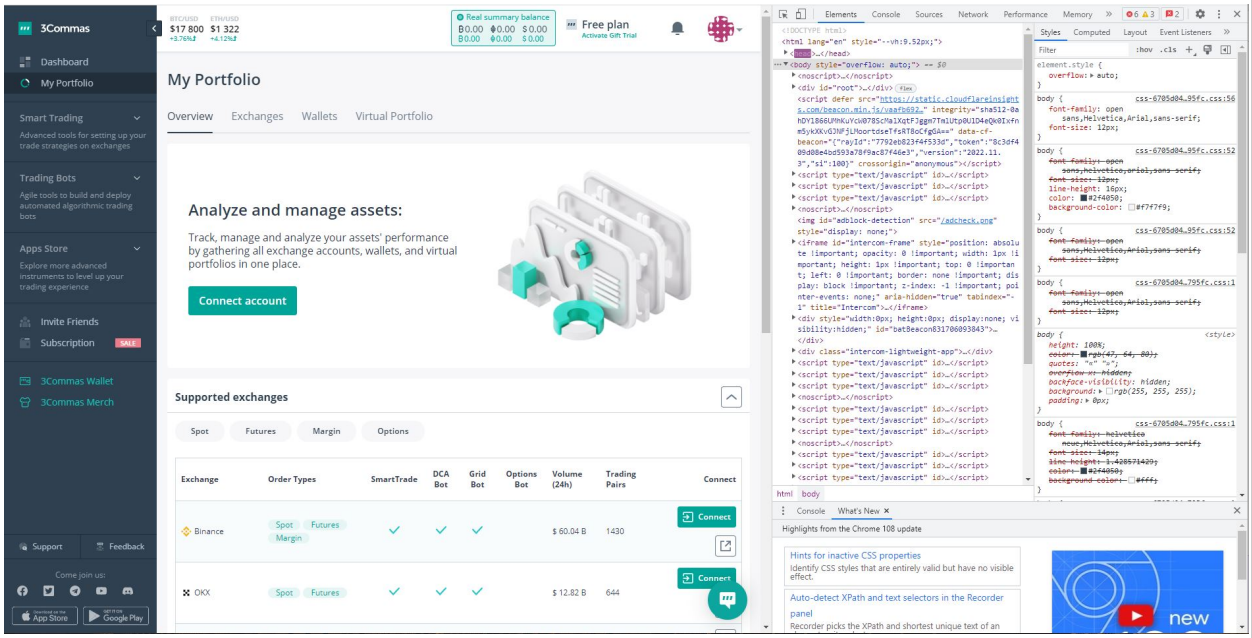
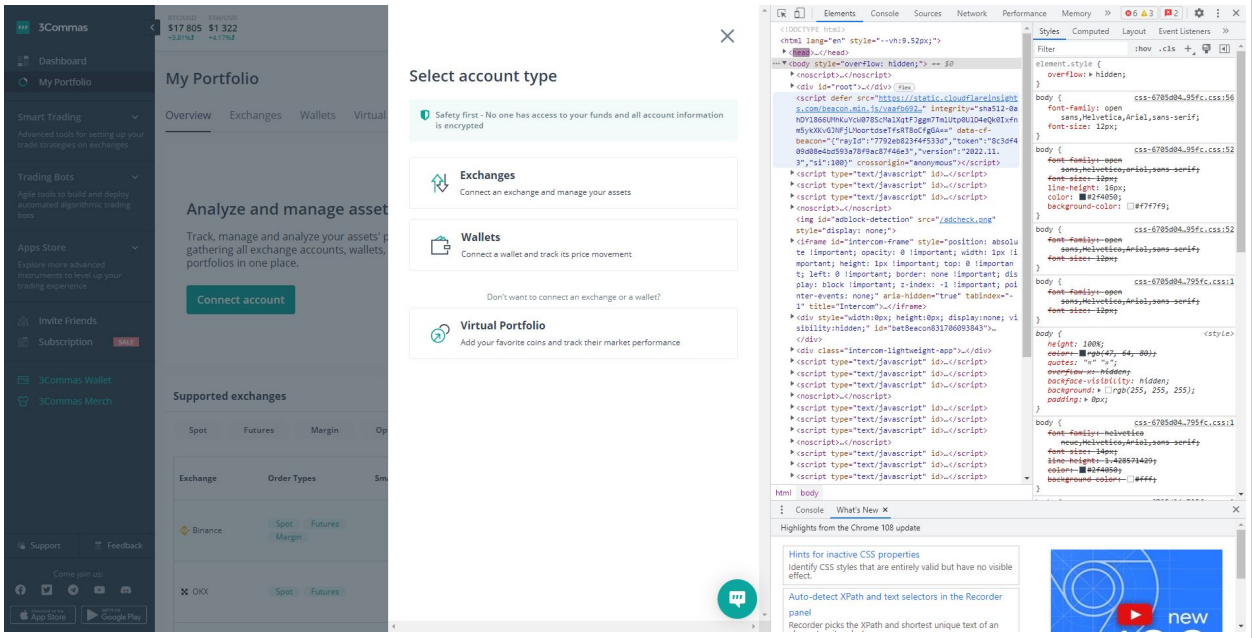


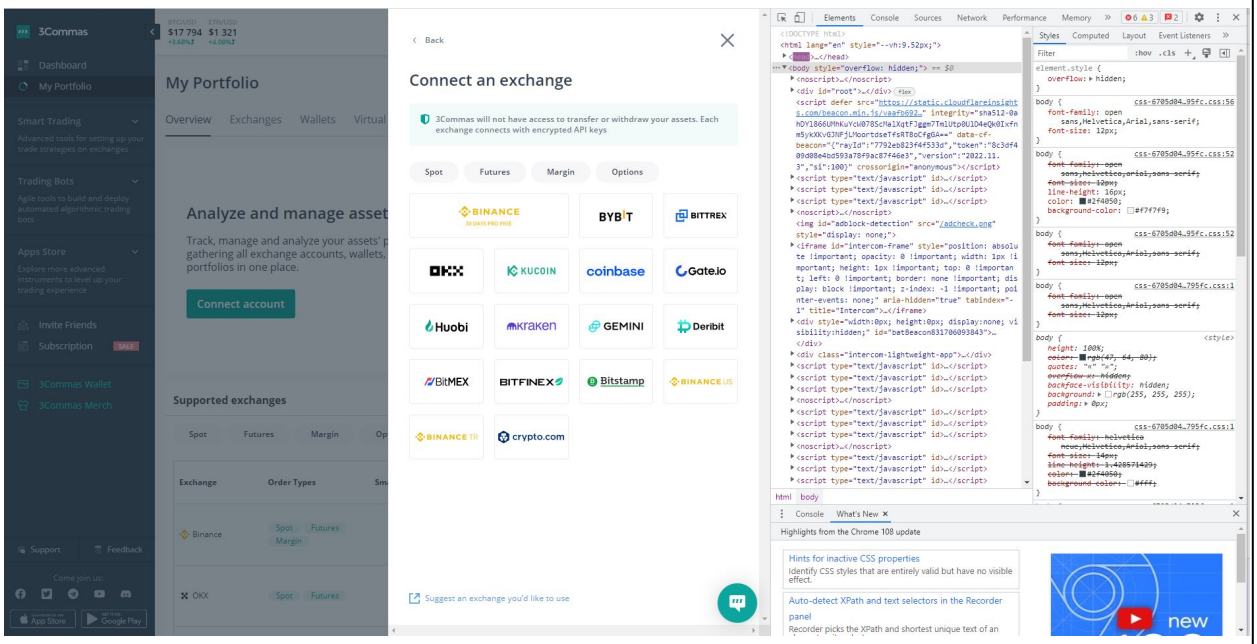
Figure 7
3Commas My Portfolio Webpage after Clicking "Connect Account"



[34] Developer Tools are a set of tools within the Google Chrome browser that allows a user to access and view a websites code, along with certain data stored within that code. They can be accessed by clicking the three horizontal dots located at the top-right of the browser window, or by pressing Ctrl + Shift +I.

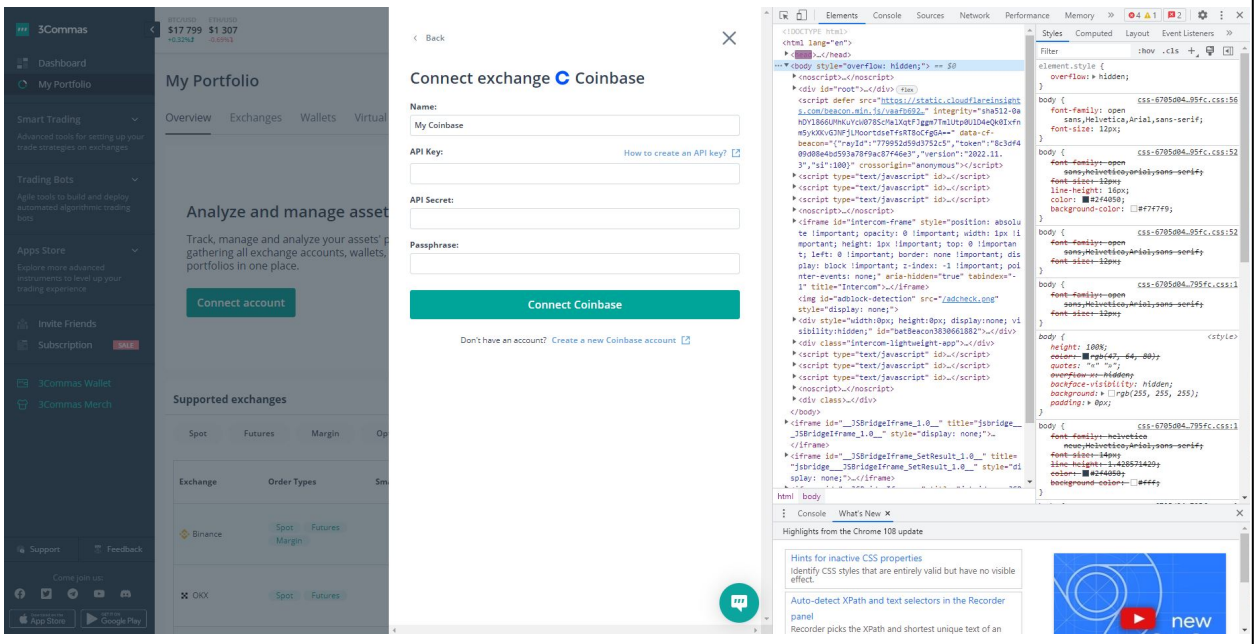
WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

Figure 8
3Commas My Portfolio Webpage displaying Cryptocurrency Platform Options



34. After selecting an exchange to connect to, the webpage will then prompt a user to enter their sensitive information – including their API key, API Secret and Passphrase. *See Figure 9* below.

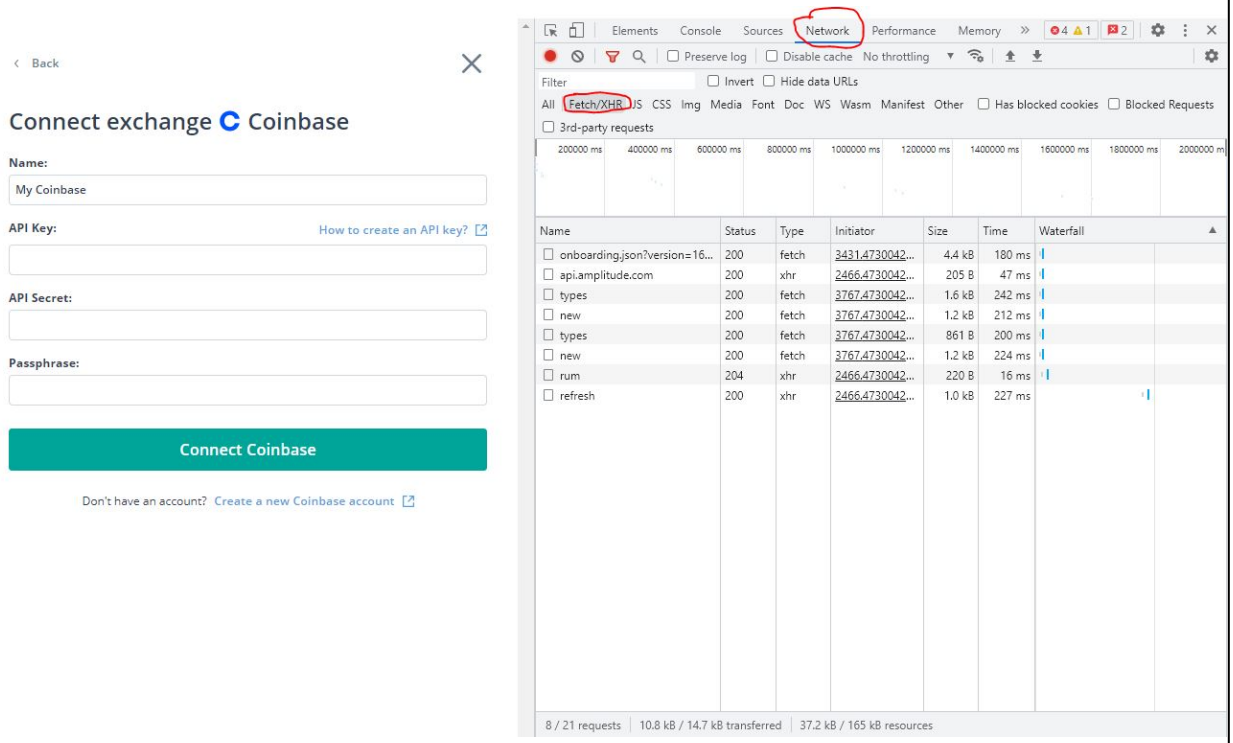
Figure 9
3Commas My Portfolio Webpage Credential Prompt



WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

35. At this time, a user can navigate to the "Network" tab in their open Developer Tool and select the "Fetch/XHR" data type. *See Figure 10* below.

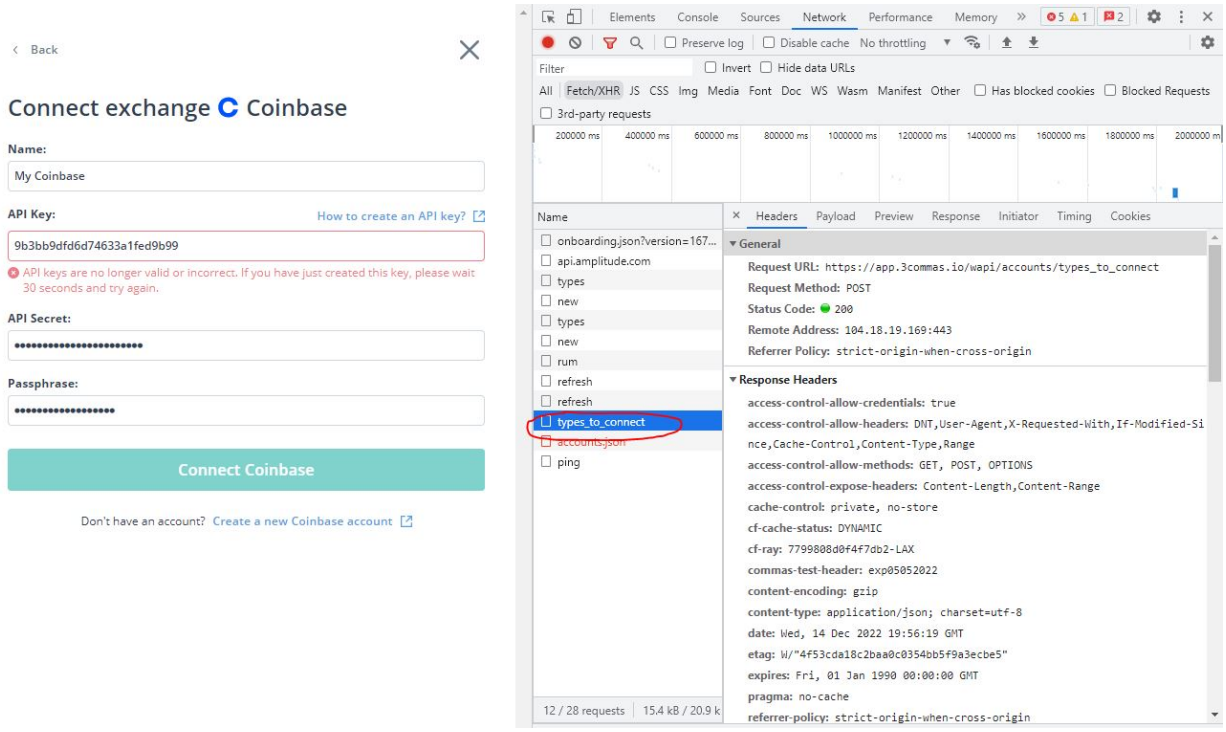
Figure 10
Connect Exchange Network Tab with Fetch/XHR Data Type Selected



WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

36. Entering any API data [35] into prompted fields on the webpage and pressing the "Connect" button will cause the "types_to_connect" data element to appear. *See Figure 11* below.

Figure 11
"types_to_connect" appearing after entering sensitive API data

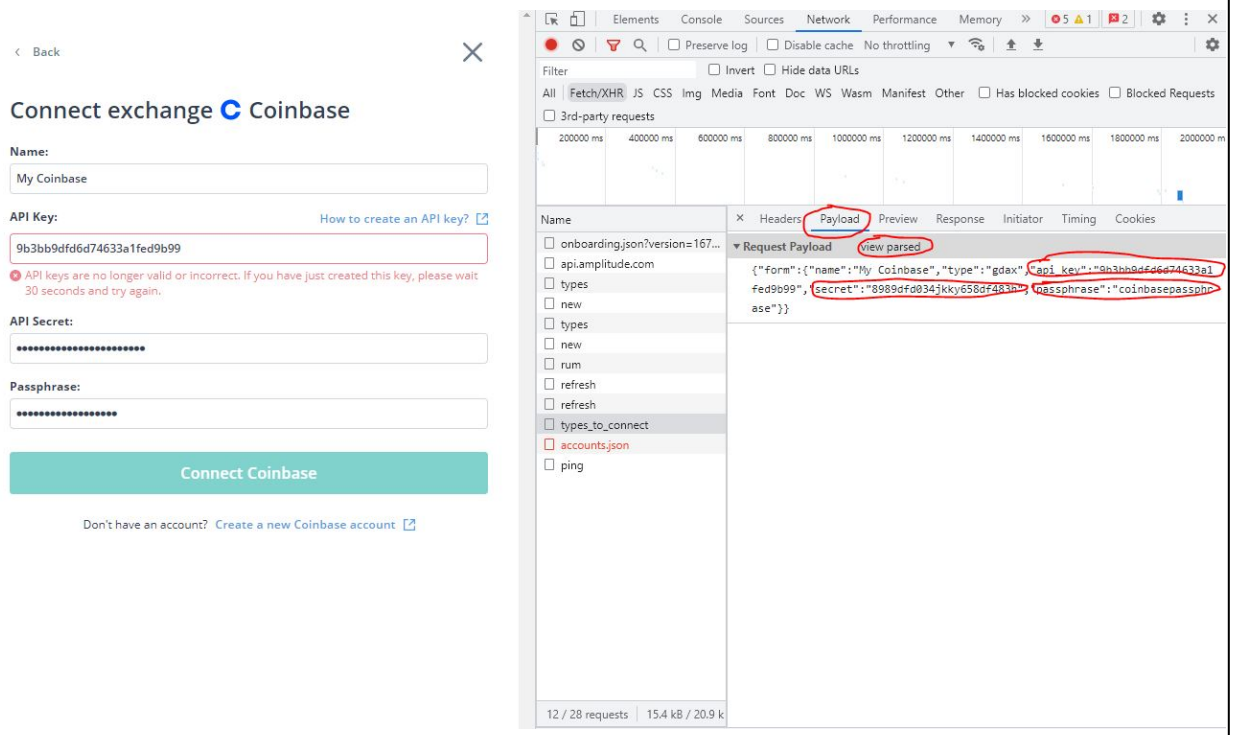


[35] Any API credentials used as examples in this Complaint are not real or valid.

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

37. By selecting the "types_to_connect" data element, clicking on the "Payload" tab, and then selecting "view source," a user will be able to view all of the sensitive API data that they entered into the 3Commas website in plain text, without **any encryption**. *See Figure 12* below.

Figure 12
"Payload" Tab Displays Sensitive API Data in Plaintext



38. This demonstrates that the 3Commas website transmits a user's sensitive API information, such as their API key, API Secret and Passphrase, to its own servers in **an unencrypted, plaintext format**. This means that any individual –whether a 3Commas employee or nefarious actor – with access to 3Commas' webservers can easily view the sensitive API data of 3Commas customers. And again, this data entry is required to utilize 3Commas' services. It is further possible that third-party services installed on the 3Commas website, such as Google Analytics, Facebook Pixel, or 3Commas' webhost Cloudflare may also be able to view the unencrypted API data that is transmitted through the 3Commas website.

39. Importantly, 3Commas' transmitting of sensitive data such as a user's API key, API Secret and Passphrase in an unencrypted, plaintext format is in direct contravention to data security best practices. Encryption protects information from unauthorized use and modification during transmission and at rest, and its implementation is listed as a security standard by the

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

National Institute of Standards and Technology for companies such as Defendant that handle sensitive information. *See, e.g.*, NIST 800-53rev.5, SC-8.

40. Further, 3Commas' lack of encryption contradicts its representations made in its public-facing Privacy Policy, which states: "[w]e have taken necessary technical and organizational security measures to protect your personal data against accidental or unlawful destruction, loss, or alteration and against the unauthorized disclosure, abuse or other processing in violation of applicable law."[36]

41. 3Commas, by failing to encrypt customers' sensitive API data and, worse, transmitting this unencrypted data, created data security vulnerabilities ripe for abuse by nefarious actors. Any hacker able to access 3Commas' servers could have exploited this lapse in security to obtain unencrypted API data without ever having to rely on a phishing scheme aimed at individual customers.

THE PARTIES

42. Plaintiff Charles Freeman is a California citizen residing in Berkeley, California. Plaintiff Freeman is a current purchaser of 3Commas' Starter Plan and has purchased 3Commas' Pro Plan in the past. Plaintiff Freeman has a KuCoin account linked to his 3Commas account. On or around December 13, 2022, Plaintiff Freeman suffered an API attack wherein numerous unauthorized trades were conducted on one of his linked KuCoin accounts. As a result of that attack, Plaintiff Freeman has suffered damages approximating $5,300.00.

43. Plaintiff Tigran Melkonyan is a California citizen residing in Los Angeles, California. Plaintiff Melkonyan is a current purchaser of 3Commas' Pro Plan and has two Coinbase Pro accounts linked to his 3Commas account. On or around November 8 or 9, 2022, Plaintiff Melkonyan suffered an API attack wherein numerous unauthorized trades were conducted on one of his linked Coinbase Pro accounts. As a result of that attack, Plaintiff Melkonyan has suffered damages approximating $269,000.00, including transaction fees of approximately $23,247.72 for the total volume of fraudulent transactions.

[36] "Privacy Policy" https://3commas.io/privacy-policy (last accessed December 14, 2022).

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

44. Plaintiff Ari Shofet is a California citizen residing in Los Angeles, California. Plaintiff Shofet is a current purchaser of 3Commas' Starter Plan and has a Coinbase Pro account linked to his 3Commas account. On or around November 24, 2022, Plaintiff Shofet suffered an API attack wherein numerous unauthorized trades were conducted on his linked Coinbase Pro account. As a result of that attack, Plaintiff Shofet has suffered damages approximating $148,336.63, including transaction fees of approximately $24,213.02 for the total volume of fraudulent transactions.

45. Plaintiff Shawn Mall is a Nevada citizen residing in Henderson, Nevada. Plaintiff is a current purchaser of 3Commas' Advanced Plan and has a Coinbase Pro account linked to his 3Commas account. On or around November 24, 2022, Plaintiff Mall suffered an API attack wherein numerous unauthorized trades were conducted on his linked Coinbase Pro account. As a result of that attack, Plaintiff Mall has suffered damages approximating $142,968.00, including transaction fees of approximately $25,753.61 for the total volume of fraudulent transactions.

46. Plaintiff Benjamin Ferris is a Washington citizen residing in Kirkland, Washington. Plaintiff Ferris is a current purchaser of 3Commas' Pro Plan and has a Coinbase Pro account linked to his 3Commas account. In late 2022, Plaintiff Ferris suffered an API attack wherein numerous unauthorized trades were conducted on his linked Coinbase Pro account. As a result of that attack, Plaintiff Ferris has suffered damages approximating $153,000.00.

47. Plaintiff Bryan Chapman is a Utah citizen residing in Saratoga Springs, Utah. Plaintiff Chapman is a current purchaser of 3Comma's Pro Plan and has a KuCoin account linked to his 3Commas account. On or around November 10, 2022, Plaintiff Chapman suffered an API attack wherein numerous unauthorized trades were conducted on his linked KuCoin account. As a result of that attack, Plaintiff Chapman has suffered damages approximating $275,000.00, including transaction fees of approximately $13,750 for the total volume of fraudulent transactions.

48. Plaintiff Nandan Arora is a Texas citizen residing in Austin, Texas. Plaintiff Arora is a current purchaser of 3Commas' Advanced Plan and has a Coinbase Pro account linked to his 3Commas account. In late 2022, Plaintiff Arora suffered an API attack wherein numerous

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

unauthorized trades were conducted on his linked Coinbase Pro account. As a result of that attack, Plaintiff Arora has suffered damages approximating $200,000.00.

49. Plaintiff Shafiq Rajani is an Illinois citizen residing in Chicago, Illinois. Plaintiff Rajani is a current purchaser of a 3Commas' paid plan and has a Coinbase Pro account linked to his 3Commas account. On or around November 25, 2022, Plaintiff Rajani suffered an API attack wherein numerous unauthorized trades were conducted on his linked Coinbase Pro account. As a result of that attack, Plaintiff Rajani has suffered damages approximating $108,000.00.

50. Plaintiff Vijay Christopher is a Michigan citizen residing in Troy, Michigan. Plaintiff Christopher is a current purchaser of 3Commas' Advanced Plan and has purchased 3Commas' Pro Plan in the past. Plaintiff Christopher has a Coinbase Pro account that was linked to his 3Commas account. On or around November 19, 2022, Plaintiff Christopher suffered an API attack wherein numerous unauthorized trades were conducted on his linked Coinbase Pro account. As a result of that attack, Plaintiff Christopher has suffered damages approximating $198.803.77, including transaction fees of approximately $18,820.64 for the total volume of fraudulent transactions.

51. Plaintiff Marc Ashby is a Pennsylvania citizen residing in Landenberg, Pennsylvania. Plaintiff Ashby is a current purchaser of 3Commas' Pro Plan and has a KuCoin account linked to his 3Commas account. On or around December 14, 2022, Plaintiff Ashby suffered an API attack wherein numerous unauthorized trade were conducted on his linked KuCoin account. As a result of that attack, Plaintiff Ashby has suffered damages approximating $14,569.70., including transaction fees of approximately $33 for the total volume of fraudulent transactions.

52. Plaintiff Vincent Van Buskirk is a New York citizen residing in New York City, New York. Plaintiff Buskirk is a current purchaser of 3Commas' Advanced Plan and has a Coinbase Pro account linked to his 3Commas account. In late 2022, Plaintiff Buskirk suffered an API attack wherein numerous unauthorized trades were conducted on his linked Coinbase Pro account. As a result of that attack, Plaintiff Buskirk has suffered damages approximating $30,000.00.

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

53. Plaintiff Lawrence Manickam is a New Jersey citizen residing in Edison, New Jersey. Plaintiff Manickam is a purchaser of 3Commas' Starter Plan and has purchased 3Commas' Pro Plan in the past. Plaintiff Manickam has a Bittrex account linked to his 3Commas account. On or around December 23, 2022, Plaintiff Manickam suffered an API attack wherein numerous unauthorized trades were conducted on his Bittrex account. As a result of that attack, Plaintiff Manickam has suffered damages approximating $49,550, including transaction fees of approximately $359 for the total volume of fraudulent transactions.

54. Plaintiff Edmundo Pena is a Florida citizen residing in Coral, Florida. Plaintiff Pena is a current purchaser of 3Commas' Pro Plan and has a Coinbase Pro account linked to his 3Commas account. In late 2022, Plaintiff Pena suffered an API attack wherein numerous unauthorized trades were conducted on his linked Coinbase Pro account. As a result of that attack, Plaintiff Pena has suffered damages approximating $59,000.00.

55. Defendant 3Commas Technologies OÜ is an Estonian private limited company with its principal address located at Harju Maakond, Tallinn, Kesklinna Linnaosa, Laeva tn2, 10111, Estonia. Estonia is a signatory to the Hauge Convention on the Service Abroad of Judicial and Extrajudicial Documents in Civil or Commercial Matters, 20 UST 361 and may be served accordingly.

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

JURISDICTION AND VENUE

56. This Court has subject matter jurisdiction over the state law claims asserted herein pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(a), as Plaintiffs are citizens of different States and Defendant is a citizen or subject of a foreign state who is not lawfully admitted for permanent residence in the United States or domiciled in any State, and the amount in controversy exceeds $75,000.

57. The Court also has personal jurisdiction over the Parties because Defendant routinely conducts business in California and has sufficient minimum contacts in California to have intentionally availed themselves to this jurisdiction by marketing and selling their Cryptocurrency Bot services in California. Further, Defendant's data server—where Defendant stores, processes and delivers data that its customers input on its website—Cloudflare, Inc., is

located and headquartered in San Francisco, California.

58. Venue is proper in this District because, among other things: (a) Plaintiff Charles Freeman is a resident of this District and a citizen of this State (b) Defendant directed its activities at residents in this District; and (c) many of the acts and omissions that give rise to this Action took place in this judicial District for services offered and purchased in this District.

59. Venue is further appropriate in this District pursuant to 28 U.S.C. § 1391 because, among other things: (a) Defendant conducts substantial business in the Northern District, (b) Plaintiff Charles Freeman resides in the Northern District, (c) Defendant directed their services at residents in the Northern District; and (d) many of the acts and omissions that give rise to this Action took place in the Northern District.

FACTUAL ALLEGATIONS

A. Plaintiffs' Experience

60. Plaintiffs and Class Members are individuals who purchased 3Commas service plans and utilized 3Commas' Bot services to make automated trades on Cryptocurrency trading platforms such as Coinbase, KuCoin, and Bittrex, among others. As a requirement of utilizing 3Commas' Bot services, Plaintiffs provided 3Commas with their sensitive API data, including their API keys, API Secret, and Passphrases.

61. Plaintiffs and Class Members purchased 3Commas service plans and provided their sensitive API data to 3Commas under the false but reasonable belief that 3Commas would implement reasonable and adequate data security safeguards to protect their sensitive API data.

62. No Plaintiff was a victim of the types of phishing that 3Commas claimed was responsible for the attacks perpetrated upon them. In particular, Plaintiff Pena is a data security expert, who keeps his device endpoints logged, recorded, and audited. At no time prior to the attack did Plaintiff Pena enter his API data into a fraudulent phishing website, nor did his data security systems detect any of his API data leaving any of his device endpoints, other than by his own input. Further, Plaintiff Pena's 3Commas account was set up approximately two and a half years ago, and Plaintiff Pena has not entered the API data associated with his 3Commas account into anything since he first linked it with his Coinbase Pro account two and a half years ago.

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

Plaintiffs did not expose their own API data and were not the victims of any phishing schemes. Plaintiffs' API data could only have been leaked or disclosed by 3Commas' breach.

B. 3Commas' Failure to Implement Reasonable and Adequate Data Security

63. 3Commas promised in its public-facing Privacy Policy that "[w]e have taken necessary technical and organizational security measures to protect your personal data against accidental or unlawful destruction, loss, or alteration and against the unauthorized disclosure, abuse or other processing in violation of applicable law."[37] 3Commas clearly recognized its duty to provide reasonable and adequate data security, such as data encryption, for Plaintiffs' and Class Members' sensitive API data. However, 3Commas failed to implement such reasonable and adequate data security safeguards as promised and instead allowed Plaintiffs' and Class Members' Personal Identifying Information ("PII"), including their sensitive API data, to be breached and utilized by nefarious third-party hackers to perpetuate attacks on their Cryptocurrency accounts.

64. In failing to implement reasonable and adequate data security, 3Commas violated federal law. Federal Trade Commission Act, 15 U.S.C. §45 prohibits 3Commas from engaging in "unfair or deceptive acts or practices affecting commerce." The Federal Trade Commission has found that a company's failure to maintain reasonable and appropriate data security for the consumers' sensitive personal information is an "unfair practice" in violation of the Federal Trade Commission Act. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236, 243 (3rd Cir. 2015).

65. In addition to their obligations under state and federal law, 3Commas owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII in their possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. 3Commas owed a duty to Plaintiffs and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that their computer system and networks, and the personnel responsible for them, adequately protected the sensitive personal information of Plaintiffs and

[37] "Privacy Policy" https://3commas.io/privacy-policy (last accessed December 14, 2022).

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

Class Members.

66. 3Commas owed a duty to Plaintiffs and Class Members to design, maintain, and test its computer system to ensure that the PII in Defendant's possession was adequately secured and protected.

67. 3Commas owed a duty to Plaintiffs and Class Members to create and implement reasonable data security practices and procedures to protect the PII in its possession, including adequately training its employees and others who accessed the PII in its possession, including adequately training its employees and others who accessed PII in its computer systems on how to adequately protect PII.

68. 3Commas owed a duty of care to Plaintiffs and Class Members to implement processes that would detect a breach of its data security systems in a timely manner.

69. 3Commas owed a duty to Plaintiffs and Class Members to act upon data security warnings and alerts in a timely fashion.

70. 3Commas owed a duty to Plaintiffs and Class Members to disclose if its computer systems and data security practices were inadequate to safeguard individuals' sensitive PII from theft because such an inadequacy would be a material fact in the decision to provide or entrust their PII to 3Commas.

71. 3Commas owed a duty to Plaintiffs and Class Members to disclose in a timely and accurate manner when their PII, including their sensitive API data, was breached.

72. 3Commas owed a duty of care to Plaintiffs and Class Members who were foreseeable and probable victims of any inadequate data security practices. 3Commas received PII from Plaintiffs and Class Members with the understanding that Plaintiffs and Class Members expected their sensitive PII to be protected from disclosure. 3Commas knew that a breach of its data systems would cause Plaintiffs and Class Members to incur substantial damages.

C. Plaintiff and Class Members Suffered Damages

73. The exposure of Plaintiff and Class Members' sensitive PII to unauthorized third-party hackers was a direct and proximate result of 3Commas' failure to properly safeguard and protect Plaintiffs' and Class Members' PII from unauthorized access, use, and disclosure, as

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

required by federal law. The data breach was also a result of 3Comma's failure to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiffs and Class Members' sensitive PII in order to protect against reasonably foreseeable threats to the security or integrity of such information, also required by federal law.

74. Plaintiffs and Class Members' PII is private and sensitive in nature and was inadequately protected by Defendant. Defendant did not obtain Plaintiffs and Class Members' consent to disclose their PII, such as their sensitive API data, except to certain persons not relevant to this action, as required by applicable law and industry standards.

75. As a direct and proximate result of Defendant's wrongful actions and inaction, and the resulting data breach, Plaintiffs and Class Members have suffered damages. Plaintiffs and Class Members are all customers of 3Commas' Bot services who had their sensitive API data breached by 3Commas and who suffered API attacks on their Crypto accounts. As a result, Plaintiffs' accounts were fraudulently used to make mass unauthorized Crypto trades in quick succession, causing damages of up to hundreds of thousands of dollars in monetary losses for each Plaintiff.

76. Further, Plaintiffs and Class Members have suffered additional damages—some up to tens of thousands of dollars—in the form of substantial transaction fees incurred as a direct result of the numerous unauthorized and fraudulent trades conducted on their respective accounts as a result of 3Commas' leak of their API data.

77. Plaintiffs and Class Members have also lost the benefit of the bargain. Plaintiffs and Class Members, as reasonable and sophisticated cryptocurrency traders, would not have entered into agreements with 3Commas, providing their PII and sensitive API data, had they known that 3Commas would not implement reasonable security measures to protect it. Plaintiffs and Class Members are thus entitled to, at minimum, the difference in price between an automated Cryptocurrency trading service that adequately protects user PII and the Cryptocurrency trading service which they received, which does not adequately protect user PII.

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

78. Defendant's wrongful actions and inaction directly and proximately caused the breach of Plaintiffs' and Class Members' PII, including their sensitive API keys to nefarious third-party hackers, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

a. The improper disclosure and leak of their PII, including their sensitive API data;

b. The actual injury flowing from the fraudulent API attacks suffered as a result of the leak of their PII, including their sensitive API data, including any transaction fees stemming therefrom;

c. Ascertainable losses in the form of actual damages suffered as a result of the breach and the value of their time reasonably incurred to remedy or mitigate the effects of the data breach; and

d. Ascertainable losses in the form of the loss of the benefits of their bargains.

D. 3Commas' Unenforceable Forum Selection Clause

79. 3Commas' user agreement contains an unenforceable forum selection clause which reads: "[t]hese Terms of Use, the Purchase Agreement and any contractual or non-contractual disputes arising out of or in connection with the use of the Software will be governed by and in accordance with Estonian law and settled in Harju County Court (Estonia)."[38] Businesses such as Defendant, which avail themselves of California law by purposefully conducting business in California with California customers, are barred from imposing forum selection clauses, such as this one, that would force plaintiffs to waive their rights to a class action[39] and remedies under California consumer law. *See, e.g.*, *Doe 1 v. AOL, LLC*, 522 F.3d 1077 (9th Cir. 2009). Accordingly, 3Commas' forum selection clause violates public policy and is wholly unenforceable.

[38] "Terms of Use" https://3commas.io/terms-and-conditions (last accessed January 6, 2023).

[39] Notably, Estonian civil procedure does not appear to allow for representative class actions brought by private individuals.

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

CLASS ACTION ALLEGATIONS

80. Plaintiffs bring this action on their own behalf and pursuant to the Federal Rules of Civil Procedure Rule 23(a), (b)(2), (b)(3), and (c)(4). Plaintiffs intend to seek certification of the following Classes, initially defined as follows:

The Nationwide Class, initially defined as:

> All persons residing in the United States of America who purchased a 3Commas service plan and provided their PII, including their API data, to 3Commas and who subsequently had their API data breached as a result of the data breach 3Commas suffered beginning in late 2022.

The California Subclass, initially defined as:

> All persons residing in the state of California who purchased a 3Commas service plan and provided their PII, including their API data, to 3Commas and who subsequently had their API data breached as a result of the data breach 3Commas suffered beginning in late 2022.

The Nevada Subclass, initially defined as:

> All persons residing in the state of Nevada who purchased a 3Commas service plan and provided their PII, including their API data, to 3Commas and who subsequently had their API data breached as a result of the data breach 3Commas suffered beginning in late 2022.

The Washington Subclass, initially defined as:

> All persons residing in the state of Nevada who purchased a 3Commas service plan and provided their PII, including their API data, to 3Commas and who subsequently had their API data breached as a result of the data breach 3Commas suffered beginning in late 2022.

The Utah Subclass, initially defined as:

> All persons residing in the state of Utah who purchased a 3Commas service plan and provided their PII, including their API data, to 3Commas and who subsequently had their API data breached as a result of the data breach 3Commas suffered beginning in late 2022.

The Texas Subclass, initially defined as:

> All persons residing in the state of Texas who purchased a 3Commas service plan and provided their PII, including their API data, to 3Commas and who subsequently had their API data breached as a result of the data breach 3Commas suffered beginning in late 2022.

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

The Illinois Subclass, initially defined as:

> All persons residing in the state of Illinois who purchased a 3Commas service plan and provided their PII, including their API data, to 3Commas and who subsequently had their API data breached as a result of the data breach 3Commas suffered beginning in late 2022.

The Michigan Subclass, initially defined as:

> All persons residing in the state of Michigan who purchased a 3Commas service plan and provided their PII, including their API data, to 3Commas and who subsequently had their API data breached as a result of the data breach 3Commas suffered beginning in late 2022.

The Pennsylvania Subclass, initially defined as:

> All persons residing in the state of Pennsylvania who purchased a 3Commas service plan and provided their PII, including their API data, to 3Commas and who subsequently had their API data breached as a result of the data breach 3Commas suffered beginning in late 2022.

The New York Subclass, initially defined as:

> All persons residing in the state of New York who purchased a 3Commas service plan and provided their PII, including their API data, to 3Commas and who subsequently had their API data breached as a result of the data breach 3Commas suffered beginning in late 2022.

The New Jersey Subclass, initially defined as:

> All persons residing in the state of New Jersey who purchased a 3Commas service plan and provided their PII, including their API data, to 3Commas and who subsequently had their API data breached as a result of the data breach 3Commas suffered beginning in late 2022.

The Florida Subclass, initially defined as:

> All persons residing in the state of Florida who purchased a 3Commas service plan and provided their PII, including their API data, to 3Commas and who subsequently had their API data breached as a result of the data breach 3Commas suffered beginning in late 2022.

81. Excluded from each of the above Classes is Defendant, including any entity in which Defendant has a controlling interest, is a parent or subsidiary, or which is controlled by Defendant, as well as the officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns of Defendant. Also excluded are the judge and the court personnel in this

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

case and any members of their immediate families. Plaintiff reserves the right to amend the Class definitions if discovery and further investigation reveal that the Classes should be expanded or otherwise modified.

82. *Numerosity*, Fed. R. Civ. P. 23(a)(1): The members of the Classes are so numerous that the joinder of all members is impractical. The disposition of the claims of Class Members in a single action will provide substantial benefits to all parties and to the Court. The Class Members are readily identifiable from information and records in Defendant's possession, custody, or control, such as reservation receipts and confirmations.

83. *Commonality*, Fed. R. Civ. P. 23(a)(2) and (b)(3): There are questions of law and fact common to the Classes, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendant took reasonable steps and measures to safeguard Plaintiffs' and Class Members' PII, including their sensitive API data;

b. Whether Defendant violated common and statutory duties by failing to implement reasonable security procedures and practices;

c. Which security procedures should Defendant be required to implement as part of any injunctive relief ordered by the Court;

d. Whether Defendant knew or should have known of the security breach prior to its admission that the breach occurred;

e. Whether Defendant has complied with any implied contractual obligation to use reasonable security measures;

f. Whether Defendant's acts and omissions described herein give rise to a claim of negligence;

g. Whether Defendant had a duty to promptly notify Plaintiffs and Class Members that their PII, including their sensitive API data, was, or potentially could be, compromised;

h. What security measures, if any, must be implemented by Defendant to comply with its duties under state and federal law;

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

i. The nature of the relief, including equitable relief, to which Plaintiffs and Class Members are entitled; and

j. Whether Plaintiffs and Class Members are entitled to damages, civil penalties, and/or injunctive relief.

84. *Typicality*. Fed. R. Civ. P. 23(a)(3): Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' sensitive PII, including their API data, like that of every other Class Member, was misused and/or disclosed by Defendant.

85. *Adequacy of Representation*, Fed. R. Civ. P. 23(a)(4): Plaintiffs will fairly and adequately represent and protect the interests of the members of the Classes. Plaintiffs have retained competent counsel experienced in litigation of class actions, including consumer and data breach class actions, and Plaintiffs intend to prosecute this action vigorously. Plaintiffs' claims are typical of the claims of other members of the Classes and Plaintiffs have the same non-conflicting interests as the other Class Members. Therefore, the interests of the Classes will be fairly and adequately represented by Plaintiffs and their counsel.

86. *Superiority of Class Action*, Fed. R. Civ. P. 23(b)(3): A class action is superior to other available methods for the fair and efficient adjudication of this controversy since joinder of all the members of the Classes is impracticable. Furthermore, the adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudication of the asserted claims. There will be no difficulty in the management of this action as a class action.

87. Damages for any individual class member are likely insufficient to justify the cost of individual litigation so that, in the absence of class treatment, Defendant's violations of law inflicting substantial damages in the aggregate would go un-remedied.

88. Class certification is also appropriate under Fed. R. Civ. P. 23(a) and (b)(2), because Defendant has acted or refused to act on grounds generally applicable to the Classes, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Classes as a whole.

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

CAUSES OF ACTION

FIRST CAUSE OF ACTION

Negligence

(On behalf of Plaintiffs and the Nationwide Class)

89. Plaintiffs repeat and incorporate herein by reference each and every allegation contained in paragraphs 1 through 88, inclusive, of this Complaint as if set forth fully herein.

90. In 2016, the Federal Trade Commission ("FTC") updated its publication, "Protecting Personal Information: A Guide for Business," which establishes guidelines for fundamental data security principles and practices for business.[40] Among other things, the guidelines dictate businesses should protect any personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses implement an intrusion detection system to expose breaches as soon as they occur; monitor all incoming traffic for activity indicating someone is attempting to infiltrate or hack the system; monitor instances when large amounts of data are transmitted to or from the system; and have a response plan ready in the event of a breach. [41] Additionally, the FTC recommends that companies limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures. [42]

91. Defendant owed Plaintiffs and Class Members a duty of care in the handling of customers' PII, including their sensitive API data. This duty included, but was not limited to, keeping that PII secure and preventing disclosure of the PII to any unauthorized third parties. This duty of care existed independently of Defendant's contractual duties to Plaintiff and the Class

[40] Federal Trade Commission, *Protecting Personal Information: A Guide for Business* (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personalinformation.pdf.

[41] *Id*.

[42] Federal Trade Commission, *Start With Security: A Guide for Business* (Jun. 2015) https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

Members. Under the FTC Guidelines, and other sources of industry-wide cybersecurity standards, Defendant is obligated to incorporate adequate measures to safeguard and protect PII that is entrusted to them in their ordinary course of business and transactions with customers.

92. Pursuant to the Federal Trade Commission Act (15 U.S.C. §45), Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs and Class Members' PII. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer information, treating the businesses' failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45. Orders from these actions further clarify the measures businesses are required to undertake in order to satisfy their data security obligations. [43]

93. Additional industry guidelines which provide a standard of care can be found in the National Institute of Standards and Technology's ("NIST's") *Framework for Improving Critical Infrastructure Cybersecurity* (Apr. 16, 2018), https://nvlpubs. nist. gov/nistpubs/CSWP/ NIST. CSWP. 04162018. pdf. Among other guideposts, the NIST's framework identifies seven steps for establishing or improving a cybersecurity program (section 3. 2). Those steps are:

> *Step 1: Prioritize and Scope*. The organization identifies its business/mission objectives and high-level organizational priorities. With this information, the organization makes strategic decisions regarding cybersecurity implementations and determines the scope of systems and assets that support the selected business line or process. The Framework can be adapted to support the different business lines or processes within an organization, which may have different business needs and associated risk tolerance. Risk tolerances may be reflected in a target Implementation Tier.

[43] Federal Trade Commission, *Privacy and Security Enforcement: Press Releases*, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-securityenforcement (last visited Nov. 22, 2019).

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

Step 2: Orient. Once the scope of the cybersecurity program has been determined for the business line or process, the organization identifies related systems and assets, regulatory requirements, and overall risk approach. The organization then consults sources to identify threats and vulnerabilities applicable to those systems and assets.

Step 3: Create a Current Profile. The organization develops a Current Profile by indicating which Category and Subcategory outcomes from the Framework Core are currently being achieved. If an outcome is partially achieved, noting this fact will help support subsequent steps by providing baseline information.

Step 4: Conduct a Risk Assessment. This assessment could be guided by the organization's overall risk management process or previous risk assessment activities. The organization analyzes the operational environment in order to discern the likelihood of a cybersecurity event and the impact that the event could have on the organization. It is important that organizations identify emerging risks and use cyber threat information from internal and external sources to gain a better understanding of the likelihood and impact of cybersecurity events.

Step 5: Create a Target Profile. The organization creates a Target Profile that focuses on the assessment of the Framework Categories and Subcategories describing the organization's desired cybersecurity outcomes. Organizations also may develop their own additional Categories and Subcategories to account for unique organizational risks. The organization may also consider influences and requirements of external stakeholders such as sector entities, customers, and business partners when creating a Target Profile. The Target Profile should appropriately reflect criteria within the target Implementation Tier.

Step 6: Determine, Analyze, and Prioritize Gaps. The organization compares the Current Profile and the Target Profile to determine gaps. Next, it creates a prioritized action plan to address gaps – reflecting mission drivers, costs

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

and benefits, and risks – to achieve the outcomes in the Target Profile. The organization then determines resources, including funding and workforce, necessary to address the gaps. Using Profiles in this manner encourages the organization to make informed decisions about cybersecurity activities, supports risk management, and enables the organization to perform cost-effective, targeted improvements.

Step 7: Implement Action Plan. The organization determines which actions to take to address the gaps, if any, identified in the previous step and then adjusts its current cybersecurity practices in order to achieve the Target Profile. For further guidance, the Framework identifies example Informative References regarding the Categories and Subcategories, but organizations should determine which standards, guidelines, and practices, including those that are sector specific, work best for their needs.

94. In addition to their obligations under federal regulations and industry standards, Defendant owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII in their possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendant owed a duty to Plaintiffs and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that their computer systems and networks, and the personnel responsible for them, adequately protected the PII/PHI of Plaintiffs and Class Members.

95. Defendant owed a duty to Plaintiffs and Class Members to design, maintain, and test their internal data systems to ensure that the PII in Defendant's possession was adequately secured and protected.

96. Defendant owed a duty to Plaintiffs and Class Members to create and implement reasonable data security practices and procedures to protect the PII in its custodianship, including adequately training its employees and others who accessed PII within its computer systems on how to adequately protect PII.

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

97. Defendant owed a duty to Plaintiffs and Class Members to implement processes or safeguards that would detect a breach of their data security systems in a timely manner.

98. Defendant owed a duty to Plaintiffs and Class Members to act upon data security warnings and alerts in a timely fashion.

99. Defendant owed a duty to Plaintiffs and Class Members to timely disclose if its computer systems and data security practices were inadequate to safeguard individuals' PII from theft because such an inadequacy would be a material consideration in Plaintiffs and Class Members' decisions to entrust their PII to Defendant.

100. Defendant owed a duty to Plaintiffs and Class Members to disclose in a timely and accurate manner when data breaches occur.

101. Defendant owed a duty of care to Plaintiffs and Class Members because they were foreseeable and probable victims of any inadequate data security practices and systems. Defendant collected PII, including sensitive API data, from Plaintiff and the Class Members. Defendant knew that a breach of its data systems would cause Plaintiff and the Class Members to incur substantial financial harm through, *inter alia*, fraudulent Crypto trades made on their connected accounts.

102. Defendant breached its duties of care to safeguard and protect the PII which Plaintiffs and Class Members entrusted to it. Defendant adopted inadequate safeguards to protect the PII—including, *inter alia*, failing to encrypt API keys, API secrets, and passphrases entered into their website and storing them in plaintext format—and failed to adopt industry-wide standards set forth above in its supposed protection of the PII. Defendant failed to design, maintain, and test its computer system to ensure that the PII was adequately secured and protected, failed to create and implement reasonable data security practices and procedures, failed to implement processes that would detect a breach of its data security systems in a timely manner, failed to disclose the breach to potentially affected customers in a timely and comprehensive manner, and otherwise breached each of the above duties of care by implementing careless security procedures which led directly to the breach.

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

103. Defendant breached the duties set forth in 15 U.S.C. §45, the FTC guidelines, the NIST's Framework for Improving Critical Infrastructure Cybersecurity, and other industry guidelines. In violation of 15 U.S.C. §45, Defendant failed to implement proper data security procedures to adequately and reasonably protect Plaintiffs and Class Member's PII/PHI. In violation of the FTC guidelines, *inter alia*, Defendant did not protect the personal customer information that it keeps; failed to properly dispose of personal information that was no longer needed; failed to encrypt information stored on computer networks; lacked the requisite understanding of their network's vulnerabilities; and failed to implement policies to correct security problems. In violation of the NIST's Framework, Defendant, *inter alia*, failed to adopt sufficient resources to identity and address security gaps.

104. Defendant's failure to comply with applicable laws and regulations constitutes negligence per se.

105. As a direct and proximate result of Defendant's failure to adequately protect and safeguard the PII, Plaintiffs and Class Members suffered damages. Plaintiffs and Class Members were damaged when their API data was breached by third-party hackers, who used that data to make hundreds of fraudulent trades on their connected accounts, causing actual monetary losses up to hundreds of thousands of dollars.

106. Plaintiffs and Class Members have suffered actual injury and are entitled to damages in an amount to be proven at trial but in excess of the minimum jurisdictional requirement of this Court.

SECOND CAUSE OF ACTION

Breach of Contract

(On behalf of Plaintiffs and the Nationwide Class)

107. Plaintiffs repeat and incorporate herein by reference each and every allegation contained in paragraphs 1 through 106, inclusive, of this Complaint as if set forth fully herein.

108. Defendant solicited and invited Plaintiffs and Class Members to purchase its services, and provide it with their PII, including their sensitive API data, in order to utilize those services. Plaintiffs and Class Members accepted Defendant's offers and purchased Defendant's

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

services and provided their PII to Defendant.

109. Plaintiffs and Class Members formed contracts with Defendant at the time they purchased their services. The terms of those contracts included promises and affirmations made by Defendant, made in its Privacy Policy and elsewhere, that it would implement reasonable and adequate data security safeguards to protect their PII. Plaintiffs and Class Members, as reasonable consumers acting reasonably under the circumstances, relied upon such representations in entering those contracts and providing their PII to Defendant.

110. Plaintiffs and Class Members performed all of their obligations under their contracts with Defendant.

111. Defendant breached its contracts with Plaintiffs and Class Members by failing to implement reasonable and adequate data security safeguards to protect Plaintiffs and Class Members' PII. As a result, Plaintiffs and Class Members API data was leaked to third-party hackers and was used to conduct fraudulent trades on their respective accounts.

112. As a direct and proximate cause of Defendant's breach, Plaintiff and Class Members have suffered actual injury and are entitled to damages in an amount to be proven at trial but in excess of the minimum jurisdictional requirement of this Court.

THIRD CAUSE OF ACTION

Quasi-Contract/Unjust Enrichment

(On behalf of Plaintiffs and the Nationwide Class)

113. Plaintiffs repeat and incorporate herein by reference each and every allegation contained in paragraphs 1 through 112, inclusive, of this Complaint as if set forth fully herein.

114. Plaintiffs and Class Members purchased services from and provided their PII, including their API data, to Defendant under the reasonable but mistaken belief that Defendant had implemented reasonable and adequate data security safeguards into its website to protect their PII. Defendant made representations to Plaintiffs and Class Members that it would implement such safeguards in, *inter alia*, its Privacy Policy, which is expressly incorporated into its Terms of Use.

115. Had Plaintiffs and Class Members known that Defendant would not implement

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

such reasonable data security safeguards and/or that Defendant would not protect their PII from unauthorized disclosure, they would not have purchased Defendant's services and would not have provided their PII to Defendant.

116. As a result, Defendant was unjustly enriched by the purchase price of the services that Plaintiffs and Class Members paid. Plaintiffs and Class Members have suffered damages, and are entitled to recovery in the amount that 3Commas was unjustly enriched, to be proven at trial.

FOURTH CAUSE OF ACTION

Violation of the Consumer Legal Remedies Act,

***Cal. Civ. Code §1750, et. seq.* ("CLRA")**

(On behalf of Plaintiffs and the California Subclass)

117. Plaintiffs repeat and incorporate herein by reference each and every allegation contained in paragraphs 1 through 116, inclusive, of this Complaint as if set forth fully herein.

118. The CLRA is a comprehensive regulatory scheme that is to be liberally construed to protect consumers against unfair and deceptive business practices in connection with the conduct of businesses providing goods, property or services to consumers primarily for personal, family, or household use.

119. Defendant is a "person" as defined by Cal. Civ. Code §§ 1761(c) and 1770, and has provided "services" as defined by Civil Code §§ 1761(b) and 1770.

120. Plaintiffs and Class Members are "consumers" as defined by Civil Code §§1761(d) and 1770 and have engaged in a "transaction" as defined by Cal. Civ. Code §§ 1761(e) and 1770.

121. Defendant's acts and practices were intended to and did result in the sale of products and services to Plaintiffs and Class Members in violation of Cal. Civ. Code § 1770(a), including, *inter alia*:

a. Misrepresenting the source, sponsorship, approval or certification of goods or services;

b. Representing that goods or services have sponsorship, approval,

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

characteristics, ingredients, uses, benefits, or quantities that they do not have;

c. Representing that goods or services are of a particular standard, quality or grade, or that goods are of a particular style or model, if they are of another;

d. Advertising goods or services with intent not to sell them as advertised;

e. Representing that the subject of a transaction has been supplied in accordance with a previous transaction when it has not.

122. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers.

123. Had Defendant disclosed to Plaintiffs and Class Members that it had not implemented reasonable and adequate data security safeguards to protect their PII, Plaintiffs and Class Members would not have purchased Defendant's services and would not have provided their PII, including their sensitive API data, to Defendant. Instead, Defendant represented to Plaintiffs and Class Members that it had implemented such reasonable and adequate data security safeguards. Plaintiffs and Class Members, as reasonable consumers acting reasonably under the circumstances, reasonably relied on Defendant's misrepresentations and omissions, the truth of which they could not have discovered.

124. As a direct and proximate cause of Defendant's wrongful actions and inactions, Plaintiffs and Class Members have suffered injury, ascertainable losses of money or property, monetary and non-monetary damages, including the benefit of their bargains in purchasing Defendant's services. Plaintiffs and Class Members are entitled to and seek all monetary and non-monetary relief allowed by law, including actual damages and punitive damages, along with an order enjoining Defendant's unlawful acts and practices as described above, as well as attorneys' fees and costs.

125. In accordance with Cal. Civil Code § 1782(a), Plaintiff has provided Defendant with the requisite written notice via certified or registered mail contemporaneously with the filing of this Complaint. Plaintiffs will seek to amend the Complaint to seek relief once the requisite 30day notice period has expired to state that Plaintiffs gave Defendant proper notice.

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

FIFTH CAUSE OF ACTION

Violation of the California Customer Records Act,

Cal. Civil Code § 1798. 80 *et seq.* ("CCRA")

(On behalf of Plaintiffs and the California Subclass)

126. Plaintiffs repeat and incorporate herein by reference each and every allegation contained in paragraphs 1 through 125, inclusive, of this Complaint as if set forth fully herein.

127. Cal. Civ. Code §1798.81.5(b) requires that "[a] business that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

128. Plaintiffs and Class Members are "customer[s]" within the meaning of Cal. Civil Code §1798.80(c) and are California residents.

129. Defendant is a "business" within the meaning of Cal. Civil Code §1798. 80(a).

130. Plaintiffs and Class Members' PII constitutes "personal information" within the meaning of Cal. Civil Code § 1798.80(e).

131. Defendant violated Cal. Civ. Code § 1798.81.5(b) by failing to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect Plaintiffs' and Class Members' PII from unauthorized access, destruction, use, modification, or disclosure as evidenced by the fact that the security of Plaintiffs' and Class Members' PII was compromised and exposed to unauthorized third-party hackers and was used to facilitate numerous fraudulent trades on their respective Crypto accounts.

132. As a direct and proximate result of Defendant's violation of Cal. Civ. Code §1798.81.5(b), Plaintiffs' and Class Members' PII was compromised and exposed in connection with Defendant's data breach.

133. As a direct and proximate cause of Defendant's wrongful actions and inactions, Plaintiffs and Class Members have suffered injury, ascertainable losses of money or property, monetary and non-monetary damages, including the benefit of their bargains in purchasing

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

Defendant's services. Plaintiffs and Class Members are entitled to and seek all monetary and non-monetary relief allowed by law, including actual damages and punitive damages, along with an order enjoining Defendant's unlawful acts and practices as described above, as well as attorneys' fees and costs.

SIXTH CAUSE OF ACTION

Violation of the California Unfair Competition Law

Cal. Bus. & Prof. Code §17200, *et. seq.* ("UCL")

(On behalf of Plaintiffs and the California Subclass)

134. Plaintiffs repeat and incorporate herein by reference each and every allegation contained in paragraphs 1 through 133, inclusive, of this Complaint as if set forth fully herein.

135. Defendant is a "person" as defined under Cal. Bus. & Prof. Code §17201.

136. Defendant violated the UCL by engaging in unlawful, unfair and deceptive business acts and practices.

137. Defendant's business practices are unfair under the UCL because Defendant has acted in a manner that is immoral, unethical, oppressive, unscrupulous, and/or substantially injurious to Plaintiffs and Class Members. The exposure of Plaintiffs' and Class Members' PII, including their sensitive API data, to third parties is substantially injurious because of the significant harm that can and did result to Plaintiffs and Class Members at the hand of those third parties. Further, the impact of the practice against Plaintiffs and Class Members far outweighs any possible justification or motive on the part of Defendant. Plaintiffs and Class Members could not reasonably have avoided this injury because they relied upon Defendant's promises to protect and safeguard their PII from disclosure, as all consumers must who wish to utilize automated Crypto trading software.

138. Defendant's business practices are unlawful because they have violated, *inter alia*, the CLRA, the CCRA, and the consumer protection statutes of the states of California, Nevada, Washington, Texas, Illinois, Michigan, Pennsylvania, New York, and Florida. Defendant's business practices are also in violation of 15 U.S.C. §45, the FTC guidelines, NIST's Framework for Improving Critical Infrastructure Cybersecurity, and other industry guidelines.

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

139. Defendant's business practices are deceptive because they have a tendency to mislead reasonable consumers. Defendant assures its customers in its Privacy Policy, which is expressly incorporated into its Terms of Use, that it will implement reasonable and adequate data security safeguards in its terms of use and privacy policy. However, Defendant does not actually implement such reasonable and adequate data security safeguards. Accordingly, reasonable consumers acting reasonably under the circumstances are reasonably misled into believing that the PII that they provide Defendant will be adequately protected from unauthorized disclosure, when it will not be.

140. Plaintiffs and Class Members have suffered monetary injury in fact as a direct and proximate result of the acts of unfair competition committed by Defendant as alleged herein in an amount to be proven at trial but in excess of the minimum jurisdictional amount of this Court. Plaintiffs suffered a monetary injury when their stolen API data was acquired by third party hackers and used to conduct fraudulent trades on their connected Crypto accounts. Plaintiffs further suffered monetary injury in the loss of the benefits of their bargains.

SEVENTH CAUSE OF ACTION

Violation of the Nevada Deceptive Trade Practices Act

Nev. Rev. Stat. Ann. §§598.0903, *et seq.* ("NDTPA")

(On behalf of Plaintiffs and the Nevada Subclass)

141. Plaintiffs repeat and incorporate herein by reference each and every allegation contained in paragraphs 1 through 140, inclusive, of this Complaint as if set forth fully herein.

142. Defendant advertised, offered, or sold goods or services in Nevada and engaged in trade or commerce directly or indirectly affecting the people of Nevada.

143. Defendant engaged in deceptive trade practices in the course of its business or occupation in Nevada, in violation of Nev. Rev. Stat. Ann. §§598.0915 and 598.0923, including, *inter alia*:

a. Knowingly making a false representation as to the characteristics, uses, and benefits of goods or services for sale in violation of Nev. Rev. Stat. §598.0915(5);

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

b. Representing that goods or services for sale are of a particular standard, quality, or grade when Defendant knew or should have known that they are of another standard, quality, or grade in violation of Nev. Rev. Stat. § 598.0915(7);

c. Advertising goods or services with intent not to sell them as advertised in violation of Nev. Rev. Stat § 598.0915(9);

d. Failing to disclose a material fact in connection with the sale of goods or services in violation of Nev. Rev. Stat. § 598.0923(A)(2); and

e. Violating state and federal statutes or regulations relating to the sale of goods or services in violation of Nev. Rev. Stat. § 598.0923(A)(3).

144. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers.

145. Had Defendant disclosed to Plaintiffs and Class Members that it had not implemented reasonable and adequate data security safeguards to protect their PII, Plaintiffs and Class Members would not have purchased Defendant's services and would not have provided their PII, including their sensitive API data, to Defendant. Instead, Defendant represented to Plaintiffs and Class Members that it had implemented such reasonable and adequate data security safeguards. Plaintiffs and Class Members, as reasonable consumers acting reasonably under the circumstances, reasonably relied on Defendant's misrepresentations and omissions, the truth of which they could not have discovered.

146. Defendant knowingly and intentionally violated NDTPA, and recklessly disregarded Plaintiffs' and Class Members' rights. Defendant knew, or should have known, that it had not implemented reasonable and adequate data security safeguards to protect its customers' PII, including their sensitive API data. Despite this, Defendant did not disclose that fact to Plaintiffs and Class Members and continued to make representations that such reasonable and adequate safeguards were in place, when in fact they were not.

147. As a direct and proximate result of Defendant's deceptive trade practices, Plaintiffs and Class members have suffered and will continue to suffer injury, ascertainable losses

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

in money or property, and monetary and non-monetary damages, including the loss of their benefits of the bargain in purchasing Defendant's services. Plaintiffs and Class Members seek all monetary and non-monetary relief allowed by law, including damages, punitive damages, attorneys' fees and costs, and any and all other relief that is just and proper.

EIGHTH CAUSE OF ACTION

Violation of the Washington Consumer Protection Act

Wash. Rev. Code Ann §§19.86.020, *et. seq.* ("WCPA")

(On behalf of Plaintiffs and the Washington Subclass)

148. Plaintiffs repeat and incorporate herein by reference each and every allegation contained in paragraphs 1 through 147, inclusive, of this Complaint as if set forth fully herein.

149. Defendant is a "person," as defined by Wash. Rev. Code Ann. § 19.86.010(1).

150. Defendant advertised, offered, or sold goods or services in Washington and engaged in trade or commerce directly or indirectly affecting the people of Washington, as defined by Wash. Rev. Code Ann. § 19.86.010 (2).

151. Defendant engaged in unfair or deceptive acts or practices in the conduct of trade or commerce, in violation of Wash. Rev. Code Ann. § 19.86.020, as described herein.

152. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers.

153. Had Defendant disclosed to Plaintiffs and Class Members that it had not implemented reasonable and adequate data security safeguards to protect their PII, Plaintiffs and Class Members would not have purchased Defendant's services and would not have provided their PII, including their sensitive API data, to Defendant. Instead, Defendant represented to Plaintiffs and Class Members that it had implemented such reasonable and adequate data security safeguards. Plaintiffs and Class Members, as reasonable consumers acting reasonably under the circumstances, reasonably relied on Defendant's misrepresentations and omissions, the truth of which they could not have discovered.

154. Defendant knowingly and intentionally violated the WCPA, and recklessly disregarded Plaintiffs' and Class Members' rights. Defendant knew, or should have known, that

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

it had not implemented reasonable and adequate data security safeguards to protect its customers' PII, including their sensitive API data. Despite this, Defendant did not disclose that fact to Plaintiffs and Class Members and continued to make representations that such reasonable and adequate safeguards were in place, when in fact they were not.

155. Defendant's conduct is injurious to the public interest because it violates Wash. Rev. Code Ann. § 19.86.020, violates a statute that contains a specific legislation declaration of public interest impact, and/or injured persons and had and has the capacity to injure persons. Further, its conduct affected the public interest, including the numerous Washingtonians affected by its deceptive business practices.

156. As a direct and proximate result of Defendant's deceptive trade practices, Plaintiffs and Class members have suffered and will continue to suffer injury, ascertainable losses in money or property, and monetary and non-monetary damages, including the loss of their benefits of the bargain in purchasing Defendant's services. Plaintiffs and Class Members seek all monetary and non-monetary relief allowed by law, including damages, punitive damages, attorneys' fees and costs, and any and all other relief that is just and proper.

NINTH CAUSE OF ACTION

Violation of the Utah Consumer Sales Practices Act

Utah Code §§13-11-1, *et. seq.* ("UCPA")

(On behalf of Plaintiffs and the Washington Subclass)

157. Plaintiffs repeat and incorporate herein by reference each and every allegation contained in paragraphs 1 through 156, inclusive, of this Complaint as if set forth fully herein.

158. Defendant is a "person," as defined by Utah Code § 13-11-1(5).

159. Defendant is a "supplier," as defined by Utah Code § 13-11-1(6), because it regularly solicits, engages in, or enforces "consumer transactions," as defined by Utah Code § 13-11-1(2).

160. Defendant engaged in deceptive and unconscionable acts and practices in connection with consumer transactions, in violation of Utah Code § 13-11-4 and Utah Code § 13-11-5, as described herein.

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

161. Defendant intended to mislead Plaintiffs and Class Members and induce them to rely on its misrepresentations and omissions.

162. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers.

163. Had Defendant disclosed to Plaintiffs and Class Members that it had not implemented reasonable and adequate data security safeguards to protect their PII, Plaintiffs and Class Members would not have purchased Defendant's services and would not have provided their PII, including their sensitive API data, to Defendant. Instead, Defendant represented to Plaintiffs and Class Members that it had implemented such reasonable and adequate data security safeguards. Plaintiffs and Class Members, as reasonable consumers acting reasonably under the circumstances, reasonably relied on Defendant's misrepresentations and omissions, the truth of which they could not have discovered.

164. Defendant had a duty to disclose the above facts due to the circumstances of this case. Defendant's duty to disclose arose from, *inter alia*, its possession of exclusive knowledge regarding its lack of reasonable and adequate data security safeguards and its active concealment of its lack of reasonable and adequate data security safeguards.

165. Defendant knowingly and intentionally violated the UCPA by, inter alia:

a. Indicating that the subject of a consumer transaction has sponsorship, approval, performance characteristics, accessories, uses, or benefits, if it has not;

b. Indicating that the subject of a consumer transaction is of a particular standard, quality, grade, style, or model, if it is not;

c. Indicating that the subject of a consumer transaction has been supplied in accordance with a previous representation, if it has not;

d. Indicating that the subject of a consumer transaction will be supplied in greater quantity (*e.g.*, more data security) than the supplier intends.

166. Defendant engaged in unconscionable acts and practices that were oppressive and led to unfair surprise, as shown in the setting, purpose, and effect of those acts and practices.

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

167. In addition, there was an overall imbalance in the obligations and rights imposed by the consumer transactions in question, based on the mores and industry standards of the time and place where they occurred. There is a substantial imbalance between the obligations and rights of consumers, such as Plaintiffs and Class Members, who purchase services based upon publicly available information, including information publicly disseminated by Defendant themselves, and Defendant, who has exclusive knowledge of any defects in their data security safeguards.

168. Defendant's acts and practices were also procedurally unconscionable because consumers, including Plaintiff and Class Members, had no practicable option but to purchase Defendant's services—which it claims to be the best and most advanced of its kind—based upon publicly-available information, despite Defendant's omissions and misrepresentations. Defendant exploited this imbalance in power, and the asymmetry of information, to profit by selling its services with the promise of reasonable and adequate data security safeguards, but without in fact implementing such safeguards.

169. As a direct and proximate result of Defendant's unconscionable and deceptive trade acts or practices, Plaintiffs and Class Members have suffered and will continue to suffer injury, ascertainable losses in money or property, and monetary and non-monetary damages, including the loss of their benefits of the bargain in purchasing Defendant's services. Plaintiffs and Class Members seek all monetary and non-monetary relief allowed by law, including actual damages, statutory damages of $2,000 per violation, injunctive relief, attorneys' fees and costs, and any and all other relief that is just and proper.

TENTH CAUSE OF ACTION

Violation of the Texas Deceptive Trade Practices – Consumer Protection Act

Tex. Bus. & Com. Code §§17.41, *et. seq.* ("TDTPA")

(On behalf of Plaintiffs and the Texas Subclass)

170. Plaintiffs repeat and incorporate herein by reference each and every allegation contained in paragraphs 1 through 169, inclusive, of this Complaint as if set forth fully herein.

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

171. Defendant is a "person," as defined by Tex. Bus. & Com. Code § 17.45(3).

172. Plaintiffs and Class Members are members are "consumers," as defined by Tex. Bus. & Com. Code § 17.45(4).

173. Defendant advertised, offered, or sold goods or services in Texas and engaged in trade or commerce directly or indirectly affecting the people of Texas, as defined by Tex. Bus. & Com. Code § 17.45(6).

174. Defendant engaged in false, misleading, or deceptive acts and practices, in violation of Tex. Bus. & Com. Code § 17.46(b), including, *inter alia*:

a. Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits or quantities that they do not have;

b. Representing that goods or services are of a particular standard, quality or grade, if they are of another; and

c. Advertising goods or services with intent not to sell them as advertised.

175. Defendant intended to mislead Plaintiffs and Texas Subclass members and induce them to rely on its misrepresentations and omissions.

176. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers.

177. Had Defendant disclosed to Plaintiffs and Class Members that it had not implemented reasonable and adequate data security safeguards to protect their PII, Plaintiffs and Class Members would not have purchased Defendant's services and would not have provided their PII, including their sensitive API data, to Defendant. Instead, Defendant represented to Plaintiffs and Class Members that it had implemented such reasonable and adequate data security safeguards. Plaintiffs and Class Members, as reasonable consumers acting reasonably under the circumstances, reasonably relied on Defendant's misrepresentations and omissions, the truth of which they could not have discovered.

178. Defendant engaged in unconscionable actions or courses of conduct, in violation of Tex. Bus. & Com. Code §17.50(a)(3). Defendant engaged in acts or practices which, to consumer's detriment, took advantage of consumer's lack of knowledge, ability, experience, or

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

capacity to a grossly unfair degree.

179. Consumers, including Plaintiffs and Class members, lacked knowledge about the deficiencies in Defendant's data security because this information was known exclusively by Defendant. Defendant took advantage of its exclusive knowledge and actively concealed the fact that its data security was not reasonable or adequate to its customers, including Plaintiffs and Class Members.

180. Defendant intended to take advantage of consumers' lack of knowledge, ability, experience, or capacity to a grossly unfair degree, with reckless disregard for the unfairness that would result. The unfairness resulting from Defendant's conduct is glaringly noticeable, flagrant, complete, and unmitigated. The data breach, which resulted from Defendant's failure to secure its own systems, exposed Plaintiffs' and Class Members' PII, including their sensitive API data, to unauthorized third-party hackers. Plaintiffs' and Class Members' exposed API data was subsequently used to make numerous fraudulent trades on their respective Crypto accounts—resulting in actual monetary losses of up to hundreds of thousands of dollars. Plaintiffs and Class Members cannot mitigate this unfairness because they cannot undo the data breach and cannot recover the entirety of their lost assets.

181. Defendant's violations present a continuing risk to Plaintiffs and Class Members, as well as to the general public. Plaintiffs and Class Members continue to wish to utilize Defendant's automatic Crypto trading services, but are now unable to determine if, or when, Defendant actually implements the reasonable and adequate data security it promises to its customers such that any further API data that they provide to Defendant will be protected.

182. As a direct and proximate result of Defendant's deceptive trade practices, Plaintiffs and Class members have suffered and will continue to suffer injury, ascertainable losses in money or property, and monetary and non-monetary damages, including the loss of their benefits of the bargain in purchasing Defendant's services. Plaintiffs and Class Members seek all monetary and non-monetary relief allowed by law, including damages, punitive damages, attorneys' fees and costs, and any and all other relief that is just and proper.

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

ELEVENTH CAUSE OF ACTION

Violation of the Illinois Uniform Deceptive Trade Practices Act

815 ILCS §§510/2, *et. seq.* ("IUDTPA")

(On behalf of Plaintiffs and the Illinois Subclass)

183. Plaintiffs repeat and incorporate herein by reference each and every allegation contained in paragraphs 1 through 182, inclusive, of this Complaint as if set forth fully herein.

184. Defendant is a "person" as defined by 815 ILCS §§ 510/1(5).

185. Defendant engaged in deceptive trade practices in the conduct of its business, in violation of 815 ILCS §§ 510/2(a), including, *inter alia*:

a. Representing that goods or services have characteristics that they do not have;

b. Representing that goods or services are of a particular standard, quality, or grade if they are of another;

c. Advertising goods or services with intent not to sell them as advertised; and

d. Engaging in other conduct that creates a likelihood of confusion or misunderstanding.

186. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers.

187. Had Defendant disclosed to Plaintiffs and Class Members that it had not implemented reasonable and adequate data security safeguards to protect their PII, Plaintiffs and Class Members would not have purchased Defendant's services and would not have provided their PII, including their sensitive API data, to Defendant. Instead, Defendant represented to Plaintiffs and Class Members that it had implemented such reasonable and adequate data security safeguards. Plaintiffs and Class Members, as reasonable consumers acting reasonably under the circumstances, reasonably relied on Defendant's misrepresentations and omissions, the truth of which they could not have discovered.

188. Defendant's unfair and deceptive acts and practices were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and Class Members that they could not reasonably avoid. These substantial injuries outweigh any benefits to

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

consumers or to competition.

189. As a direct and proximate result of Defendant's deceptive trade practices, Plaintiffs and Class members have suffered and will continue to suffer injury, ascertainable losses in money or property, and monetary and non-monetary damages, including the loss of their benefits of the bargain in purchasing Defendant's services. Plaintiffs and Class Members seek all monetary and non-monetary relief allowed by law, including damages, punitive damages, attorneys' fees and costs, and any and all other relief that is just and proper.

TWELTH CAUSE OF ACTION

Violation of the Michigan Consumer Protection Act

Mich. Comp. Laws. Ann. §§445.903, *et. seq.* ("MCPA")

(On behalf of Plaintiffs and the Michigan Subclass)

190. Plaintiffs repeat and incorporate herein by reference each and every allegation contained in paragraphs 1 through 189, inclusive, of this Complaint as if set forth fully herein.

191. Defendant and Michigan Subclass members are "persons" as defined by Mich. Comp. Laws Ann. § 445.903(d).

192. Defendant advertised, offered, or sold goods or services in Michigan and engaged in trade or commerce directly or indirectly affecting the people of Michigan, as defined by Mich. Comp. Laws Ann. § 445.903(g).

193. Defendant engaged in unfair, unconscionable, and deceptive practices in the conduct of trade and commerce, in violation of Mich. Comp. Laws Ann. § 445.903(1), including, *inter alia*:

a. Representing that its goods and services have characteristics, uses, and benefits that they do not have;

b. Representing that its goods and services are of a particular standard or quality if they are of another;

c. Making a representation or statement of fact material to the transaction such that a person reasonably believes the represented or suggested state of affairs to be other than it actually is; and

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

d. Failing to reveal facts that are material to the transaction in light of representations made in a positive manner.

194. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers.

195. Had Defendant disclosed to Plaintiffs and Class Members that it had not implemented reasonable and adequate data security safeguards to protect their PII, Plaintiffs and Class Members would not have purchased Defendant's services and would not have provided their PII, including their sensitive API data, to Defendant. Instead, Defendant represented to Plaintiffs and Class Members that it had implemented such reasonable and adequate data security safeguards. Plaintiffs and Class Members, as reasonable consumers acting reasonably under the circumstances, reasonably relied on Defendant's misrepresentations and omissions, the truth of which they could not have discovered.

196. Defendant intended to mislead Plaintiffs and Class Members and induce them to rely on its misrepresentations and omissions.

197. Defendant knowingly and intentionally violated MCPA, and recklessly disregarded Plaintiffs' and Class Members' rights. Defendant knew, or should have known, that it had not implemented reasonable and adequate data security safeguards to protect its customers' PII, including their sensitive API data. Despite this, Defendant did not disclose that fact to Plaintiffs and Class Members and continued to make representations that such reasonable and adequate safeguards were in place, when in fact they were not.

198. As a direct and proximate result of Defendant's deceptive trade practices, Plaintiffs and Class members have suffered and will continue to suffer injury, ascertainable losses in money or property, and monetary and non-monetary damages, including the loss of their benefits of the bargain in purchasing Defendant's services. Plaintiffs and Class Members seek all monetary and non-monetary relief allowed by law, including the greater of actual damages or $250, and any and all other relief that is just and proper.

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

THIRTEENTH CAUSE OF ACTION

Violation of the Pennsylvania Unfair Trade Practices and Consumer Protection Law

73 Pa. Cons. Stat. §§201-2 & 201-3, *et. seq.* ("UTPCPL")

(On behalf of Plaintiffs and the Pennsylvania Subclass)

199. Plaintiffs repeat and incorporate herein by reference each and every allegation contained in paragraphs 1 through 198, inclusive, of this Complaint as if set forth fully herein.

200. Defendant is a "person," as meant by 73 Pa. Cons. Stat. § 201-2(2).

201. Plaintiff and Pennsylvania Subclass members purchased goods and services in "trade" and "commerce," as defined under Pa. Cons. Stat. § 201-2(3), primarily for personal, family, and/or household purposes.

202. Defendant engaged in unfair methods of competition and unfair or deceptive acts or practices in the conduct of its trade and commerce in violation of 73 Pa. Cons. Stat. Ann. § 201-3, including, *inter alia*:

a. Representing that its goods and services have characteristics, uses, benefits, and qualities that they do not have;

b. Representing that its goods and services are of a particular standard or quality if they are another; and

c. Advertising its goods and services with intent not to sell them as advertised.

203. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers.

204. Had Defendant disclosed to Plaintiffs and Class Members that it had not implemented reasonable and adequate data security safeguards to protect their PII, Plaintiffs and Class Members would not have purchased Defendant's services and would not have provided their PII, including their sensitive API data, to Defendant. Instead, Defendant represented to Plaintiffs and Class Members that it had implemented such reasonable and adequate data security safeguards. Plaintiffs and Class Members, as reasonable consumers acting reasonably under the circumstances, reasonably relied on Defendant's misrepresentations and omissions, the truth of which they could not have discovered.

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

205. Defendant intended to mislead Plaintiffs and Class Members and induce them to rely on its misrepresentations and omissions.

206. Defendant knowingly and intentionally violated UTPCPL, and recklessly disregarded Plaintiffs' and Class Members' rights. Defendant knew, or should have known, that it had not implemented reasonable and adequate data security safeguards to protect its customers' PII, including their sensitive API data. Despite this, Defendant did not disclose that fact to Plaintiffs and Class Members and continued to make representations that such reasonable and adequate safeguards were in place, when in fact they were not.

207. As a direct and proximate result of Defendant's deceptive trade practices, Plaintiffs and Class members have suffered and will continue to suffer injury, ascertainable losses in money or property, and monetary and non-monetary damages, including the loss of their benefits of the bargain in purchasing Defendant's services. Plaintiffs and Class Members seek all monetary and non-monetary relief allowed by law, including the greater of actual damages or $100, and any and all other relief that is just and proper.

FOURTEENTH CAUSE OF ACTION

Violation of New York General Business Law

N.Y. Gen. Bus. Law §§349 and 350, *et. seq.* ("GBL")

(On behalf of Plaintiffs and the New York Subclass)

208. Plaintiffs repeat and incorporate herein by reference each and every allegation contained in paragraphs 1 through 207, inclusive, of this Complaint as if set forth fully herein.

209. Defendant engaged in deceptive acts or practices in the conduct of its business, trade, and commerce or furnishing of services, in violation of N.Y. Gen. Bus. Law §§ 349 and 350. Specifically, Defendant made false and material promises to its customers that it had implemented reasonable and adequate data security safeguards to protect their PII, including their sensitive API data. Defendant made those promises in, *inter alia*, its Privacy Policy, which was expressly incorporated into its Terms of Use. Which stated that "[w]e have taken necessary technological and organizational security measures to protect your personal data against accidental or unlawful destruction, loss or alteration and against the unauthorized disclosure,

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

abuse or other processing in violation of applicable law."

210. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers acting reasonably under the circumstances.

211. Had Defendant disclosed to Plaintiffs and Class Members that it had not implemented reasonable and adequate data security safeguards to protect their PII, Plaintiffs and Class Members would not have purchased Defendant's services and would not have provided their PII, including their sensitive API data, to Defendant. Instead, Defendant represented to Plaintiffs and Class Members that it had implemented such reasonable and adequate data security safeguards. Plaintiffs and Class Members, as reasonable consumers acting reasonably under the circumstances, reasonably relied on Defendant's misrepresentations and omissions, the truth of which they could not have discovered.

212. Defendant's false and material promises constitute unlawful "false advertising in the conduct of [any] business trade or commerce in the furnishing of any service" in violation of N.Y. Gen. Bus. Law §350.

213. Defendant knowingly and intentionally violated GBL, and recklessly disregarded Plaintiffs' and Class Members' rights. Defendant knew, or should have known, that it had not implemented reasonable and adequate data security safeguards to protect it customers' PII, including their sensitive API data. Despite this, Defendant did not disclose that fact to Plaintiffs and Class Members and continued to make representations that such reasonable and adequate safeguards were in place, when in fact they were not.

214. Defendant's deceptive and unlawful acts and practices complained of herein affected the public interest and consumers at large, including the numerous New York residents who purchased Defendant's services.

215. The above-described deceptive and unlawful practices and acts by Defendant caused substantial injury to Plaintiff and Class Members that they could not have reasonably avoided. Defendant was, at all times prior to the data breach, in exclusive possession of the knowledge that its data security safeguards were not reasonable or adequate. Plaintiffs and Class Members could not have reasonably discovered that Defendant's data security safeguards were

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

not reasonable and adequate prior to the breach occurring.

216. As a direct and proximate result of Defendant's deceptive trade practices, Plaintiffs and Class members have suffered and will continue to suffer injury, ascertainable losses in money or property, and monetary and non-monetary damages, including the loss of their benefits of the bargain in purchasing Defendant's services. Plaintiffs and Class Members seek all monetary and non-monetary relief allowed by law, including the greater of actual damages or $550, treble damages, injunctive relief, attorneys' fees and costs, and any and all other relief allowable by law.

FIFTEENTH CAUSE OF ACTION

Violation of the New Jersey Consumer Fraud Act

N.J. Stat. Ann. §§56:8-1, *et. seq.* ("NJCFA")

(On behalf of Plaintiffs and the New Jersey Subclass)

217. Plaintiffs repeat and incorporate herein by reference each and every allegation contained in paragraphs 1 through 216, inclusive, of this Complaint as if set forth fully herein.

218. Defendant is a "person," as defined by N.J. Stat. Ann. § 56:8-1(d).

219. Defendant sells "merchandise," as defined by N.J. Stat. Ann. § 56:8-1(c) & (e).

220. The NJCFA prohibits unconscionable commercial practices, deception, fraud, false pretenses, false promises, misrepresentation, as well as the knowing concealment, suppression, or omission of any material fact with the intent that others rely on the concealment, omission, or fact, in connection with the sale or advertisement of any merchandise.

221. Defendant knowingly and intentionally violated NJCFA by the above-described practices, and recklessly disregarded Plaintiffs' and Class Members' rights. Defendant knew, or should have known, that it had not implemented reasonable and adequate data security safeguards to protect it customers' PII, including their sensitive API data. Despite this, Defendant did not disclose that fact to Plaintiffs and Class Members and continued to make representations that such reasonable and adequate safeguards were in place, when in fact they were not.

222. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers acting reasonably under the circumstances.

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

223. Had Defendant disclosed to Plaintiffs and Class Members that it had not implemented reasonable and adequate data security safeguards to protect their PII, Plaintiffs and Class Members would not have purchased Defendant's services and would not have provided their PII, including their sensitive API data, to Defendant. Instead, Defendant represented to Plaintiffs and Class Members that it had implemented such reasonable and adequate data security safeguards. Plaintiffs and Class Members, as reasonable consumers acting reasonably under the circumstances, reasonably relied on Defendant's misrepresentations and omissions, the truth of which they could not have discovered.

224. As a direct and proximate result of Defendant's deceptive trade practices, Plaintiffs and Class members have suffered and will continue to suffer injury, ascertainable losses in money or property, and monetary and non-monetary damages, including the loss of their benefits of the bargain in purchasing Defendant's services. Plaintiffs and Class Members seek all monetary and non-monetary relief allowed by law, treble damages, restitution and attorneys' fees and costs, as well as any and all other relief that is just and proper.

SIXTEENTH CAUSE OF ACTION

Violation of the Florida Deceptive and Unfair Trade Practices Act

Fla. Stat. §§501.201, *et. seq.* ("FDUTPA")

(On behalf of Plaintiffs and the Florida Subclass)

225. Plaintiffs repeat and incorporate herein by reference each and every allegation contained in paragraphs 1 through 224, inclusive, of this Complaint as if set forth fully herein.

226. Plaintiff and Florida Subclass members are "consumers" as defined by Fla. Stat. § 501.203.

227. Defendant advertised, offered, or sold goods or services in Florida and engaged in trade or commerce directly or indirectly affecting the people of Florida.

228. Defendant engaged in unconscionable, unfair, and deceptive acts and practices in the conduct of trade and commerce, in violation of Fla. Stat. § 501.204(1).

229. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers acting reasonably under the circumstances.

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

230. Had Defendant disclosed to Plaintiffs and Class Members that it had not implemented reasonable and adequate data security safeguards to protect their PII, Plaintiffs and Class Members would not have purchased Defendant's services and would not have provided their PII, including their sensitive API data, to Defendant. Instead, Defendant represented to Plaintiffs and Class Members that it had implemented such reasonable and adequate data security safeguards. Plaintiffs and Class Members, as reasonable consumers acting reasonably under the circumstances, reasonably relied on Defendant's misrepresentations and omissions, the truth of which they could not have discovered.

231. As a direct and proximate result of Defendant's deceptive trade practices, Plaintiffs and Class members have suffered and will continue to suffer injury, ascertainable losses in money or property, and monetary and non-monetary damages, including the loss of their benefits of the bargain in purchasing Defendant's services. Plaintiffs and Class Members seek all monetary and non-monetary relief allowed by law, including actual or nominal damages under Fla. Stat. §501.21, injunctive relief, attorneys' fees and costs, and any and all other relief allowable by law.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of all of the Class Members, respectfully requests that the Court enter judgment in her favor and against Defendant as follows:

1. For an Order certifying the Classes as defined herein and appointing Plaintiffs and their Counsel to represent the Classes;
2. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class Members' PII, including their sensitive API data, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiff and Class Members;
3. For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to API and other customer PII, storage, and safety and to disclose with specificity to Class Members the type of PII compromised.
4. For an award of actual damages, statutory damages and compensatory damages,

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

in an amount to be determined at trial;

5. For an award of punitive and treble damages, in an amount to be determined at trial;

6. For an award of costs of suit, litigation expenses and attorneys' fees, as allowable by law; and

7. For such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs, on behalf of themselves and all others similarly situated, hereby demands a jury trial for all claims so triable.

Dated: January 9, 2023

Respectfully Submitted,

/s/ *Thiago M. Coelho*
Thiago M. Coelho
WILSHIRE LAW FIRM, PLC
Attorneys for Plaintiff

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137