Vijay J. Rajagopal, State Bar No. 290886
vijay@kurichetylaw.com
KURICHETY LAW PC
179 McKnight Drive, Suite 6
Laguna Beach, California 92651
Tel: 217-390-2505

Michael Kozlowski (*pro hac vice forthcoming*)
michael.kozlowski@esbrook.com
ESBROOK PC
321 N. Clark Street Suite 1930
Chicago, Illinois 60654
Tel: (312) 319-7682

Attorneys for Plaintiff
MICHAEL MASHKEVICH, on behalf of himself and all others similarly situated

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA, SAN JOSE DIVISION

MICHAEL MASHKEVICH, on behalf of himself and all others similarly situated,

Plaintiff,

v.

UAB QBIT FINANCIAL SERVICE; BYTECHIP LLC d/b/a QBIT and QBITPAY; and YUJUN WU a/k/a MICHAEL WU,

Defendants.

Case No.

COMPLAINT FOR:

(1) CIVIL THEFT
(2) UNJUST ENRICHMENT
(3) REPLEVIN
(4) CONVERSION
(5) MONEY HAD AND RECEIVED
(6) AIDING AND ABETTING
(7) CIVIL CONSPIRACY

CLASS ACTION
DEMAND FOR JURY TRIAL

I. INTRODUCTION

Plaintiff Michael Mashkevich ("Mr. Mashkevich" or "Plaintiff"), on behalf of himself and all others similarly situated alleges as follows:

1. UAB Qbit Financial Service ("Qbit"), Bytechip LLC d/b/a/ Qbit and QbitPay ("Bytechip"), and Yujun Wu ("Wu") (collectively "Defendants") are engaged in a scheme with other individuals—sometimes identified as Olivia Ava ("Ava"), Emma Miller ("Miller"), and F.B. Lee ("Lee")[1] (collectively, and together with other unknown co-conspirators, the "Scammers")—to execute an online theft scheme known as "pig butchering," whereby they use fraudulent representations to steal large amounts of money from scores of innocent victims, including Plaintiff. The Scammers insidiously lure unsuspecting targets into buying cryptocurrency and transferring it to accounts (also known as "wallets") that they control. Once transferred, the Scammers launder the funds through a complex web of related transactions via a well-established scam network of related wallets. The victims suffer a total loss of their cryptocurrency and the funds used to purchase it. Despite the Scammer's best efforts, Plaintiff's experts from Inca Digital, a cryptocurrency investigation firm ("Inca"), traced a significant portion of the stolen funds directly to the OKX cryptocurrency exchange at address THGTenLmvqWycGLGtgRvX4wURiHQeDvNps ("the THGTen Destination Wallet" or "THGTen"). By their own admission, Qbit owns and controls this wallet. Despite their claims that the wallet is used for legitimate business purposes, overwhelming evidence suggests that, at best, Defendants received stolen funds that they knew or should have known were stolen, and, more likely, that they were active participants in the scam, deliberately providing laundering services critical to the furtherance of the scam.

2. The Scammers' pig butchering scheme here relies on confidence scams. The Scammers gain the victims' trust by feigning empathy and telling cleverly disguised lies in order to induce them to systematically increase the amount of cryptocurrency transferred to wallets under the Scammers' control. The Scammers first solicit victims by sending boilerplate inquiries about investment opportunities or part-time work. After a person responds to a message, one or more Scammers contact that person and describe the opportunities, all of which have the purported potential of earning the victim significant income by completing seemingly legitimate work tasks for well-known companies or by making seemingly legitimate investments.

[1] Ava, Miller and Lee are WhatsApp aliases used to communicate with Plaintiff in furtherance of the fraudulent scheme alleged herein.

3. The Scammers used this specious scheme to lure a common class of victims ("Class Members," or the "Class") to transfer funds to cryptocurrency wallets controlled by the Scammers. The Class in this matter is defined as all persons and entities who, at the suggestion of the Scammers or individuals acting under the Scammers' instruction or control, transferred cryptocurrency into one or more of the cryptocurrency wallets identified in Appendix A and other scam wallet addresses controlled by the Scammers as may be identified during discovery. The wallets identified on Appendix A are hereinafter referred to as "the Deposit Wallets" and are the wallets into which the Class victims transferred funds.

4. The Scammers followed a standardized roadmap to manipulate Class Members to transfer cryptocurrency to the Deposit Wallets controlled by Defendants or their co-conspirators. First, the Scammers requested that Class Members contribute a small amount of funds to set up their respective "accounts." Then the Scammers represented that Class Members had earned money and permitted Class Members to withdraw that money. The Scammers then represented that Class Members needed to transfer additional funds to their accounts for standardized, boilerplate reasons, including increasing their earning potential, their account balance had gone negative, they owed taxes, or due to a problem with loans from other investment or work platform members. After the Scammers persuaded Class Members to deposit additional cryptocurrency, they transferred it along a well-established scam cryptocurrency laundering network—controlled by Defendants or their co-conspirators—(the "Laundering Network") until it arrived at destination wallets held at cryptocurrency exchanges shown in Appendix B (the "Destination Wallets"). [2]

5. The Deposit Wallets are the initial accounts used by the Scammers to take possession of victims' cryptocurrency and the wallets into which the Class initially transferred their funds. They represent the first node of Laundering Network. The second node of the Laundering Network involves thirteen pass-through "pivot" wallets (the "Pivot Wallets"). Defendants' or their co-conspirators transferred the Class Members' stolen cryptocurrency from the Deposit Wallets to the Pivot Wallets, which served as focus points for aggregating stolen funds from multiple victims before the

[2] One or more of the Pivot Wallets were also used by the Defendants as Destination Wallets for the Class Members' transfer of cryptocurrency in the Laundering Network.

cryptocurrency was sent to various other wallets in the Laundering Network, all with the design and intent of blending and cloaking the stolen cryptocurrency in an attempt to make it appear legitimate.

6. The final node of the Laundering Network involves the reconsolidation of the stolen cryptocurrency into wallets on cryptocurrency exchanges, enabling Defendants or their co-conspirators to convert and liquidate the stolen assets. The wallets currently holding Class Members' stolen cryptocurrency, as identified in Appendix B, are used to convert the cryptocurrency into fiat currency,[3] thereby permanently placing them beyond the reach of Class Members.

7. Plaintiff is a resident of Albertville, Alabama. Like other similarly situated Class Members, Plaintiff was tricked by the Scammers, including people identifying themselves Ava, Miller, and Lee, as part of a common scheme to transfer funds to the Deposit Wallets. Plaintiff was first contacted via WhatsApp on or about March 20, 2024. The Scammers followed the standardized playbook set forth above, luring Plaintiff to transfer progressively greater amounts of cryptocurrency into Deposit Wallets. The Scammers eventually entirely blocked Plaintiff from accessing his "accounts" and transferring or withdrawing his funds.

8. After Plaintiff could not recover his funds, he contacted Inca, which traced his transactions and confirmed that Defendants were orchestrating a pig butchering confidence scheme. As described below, Inca investigated other transactions and found that these transactions were part of a common scheme to steal Class Member funds.

9. Based on Inca's investigation to date, Defendants' scheme involved transactions during the period from March 2024 through at least June 4, 2024, included thousands of Class Member victims, and involved the conversion by the Scammers of an estimated $28 million of Class Member funds. To date, the investigation initiated by Plaintiff has identified the Deposit Wallets set forth in Appendix A and the Destination Wallets set forth in Appendix B, the latter of which are categorized by cryptocurrency exchange.

[3] "Fiat currency," as used herein, refers to the type of government-issued currency, such as the U.S. dollar, that is not backed by a physical commodity, like gold or silver, or other tangible asset or commodity.

10. According to Inca's forensic analysis, it is highly likely that the owners of all the cryptocurrency wallets through which the Class Members' stolen cryptocurrency passed, starting with the Deposit Wallets, continuing to the Pivot Wallets, and eventually the Destination Wallets, were active participants in the Laundering Network. A significant portion of the stolen funds are directly traceable to the OKX cryptocurrency exchange at address THGTenLmvqWycGLGtgRvX4wURiHQeDvNps ("the THGTen Destination Wallet"), which serves a vital function in the Scam Network as an off-ramp to turn stolen assets into usable crypto- or fiat currency.

11. On, June 4, 2024, Plaintiff brought an action in the Circuit Court of Marshall County, Alabama (the "Alabama Court"), civil action number 50-CV-2024-900163.00. That same day, the Alabama Court issued a Temporary Restraining Order and Order to Show Cause, freezing the Destination Wallets set forth in Appendix B. On June 14, 2024, the Alabama Court issued its Preliminary Injunction maintaining the freeze on the Destination Wallets. A true and correct copy of both orders are attached as Exhibits A and B.

12. On January 20, 2025, Qbit filed a nonparty motion to dissolve or modify the preliminary injunction order, claiming that the court did not have jurisdiction to impose its injunction and that the funds contained in the THGTen Destination Wallet were legitimate. As evidence of Qbit's legitimacy, they relied solely on a declaration of their CEO Yujun Wu. The declaration is full of vague and conclusory statements that are demonstrably misleading and lack any documentary support.

13. Further evidence suggests the deficiencies in Qbit's motion may have been driven by their need to conceal their knowing receipt of stolen funds or active participation in laundering. Not only do Qbit and Wu hold stolen cryptocurrency that they refuse to return, but they have also been previously accused of laundering fraudulently obtained funds, resulting in the forfeiture of over $1,000,000. Finally, Inca's on chain-analysis of Qbit owned wallets strongly indicates that the wallets are used for illegitimate purposes related to cryptocurrency laundering.

14. The Alabama Court held a hearing on Qbit's motion on February 14, 2024. It could issue a decision any day to dissolve the injunction, at which point Plaintiff and Class Member funds held in THGTen would be forever beyond their reach. Accordingly, Plaintiff requests that this Court

issue an Order that recognizes the Alabama Court's June 4 and 14 orders and similarly enjoins the transfer of funds from the Defendant-controlled wallet identified in Appendix B as THGTenLmvqWycGLGtgRvX4wURiHQeDvNps as well as any other wallet owned or controlled by any Defendant.

15. Plaintiff brings this action on behalf of himself, and all others similarly situated, to recover the stolen cryptocurrency.

II. JURISDICTION, VENUE, AND ASSIGNMENT

16. This Court has personal jurisdiction over Defendant Qbit as an entity engaged in business in California and whose operations, business structure, and ownership demonstrate that it is the alter ego of Bytechip and Yujun Wu, both of which maintain substantial, continuous, and systematic contacts with California.

17. Qbit maintains an office in California at Zanker Rd. Ste 110, San Jose, CA 95131.

18. Qbit has also continuously operated, maintained offices, and conducted business in California through Bytechip and their common owner Yujun Wu.

19. Bytechip did business as Qbit and QbitPay, was owned by Qbit's executive officer, Yujun Wu, and maintained an office at the same address as Qbit: 2381 Zanker Rd, Ste 110, San Jose CA 95131. The two entities are so intertwined that Qbit should be treated as present in California for jurisdictional purposes.

20. Bytechip is subject to personal jurisdiction in California. Bytechip is a Delaware limited liability company, registered to do business in California. (California File No. 202021210840). It lists offices in California as its primary location in multiple public and legal filings. Similarly, Bytechip has affirmed its ties to the state and submitted to the jurisdiction of California's judicial system by bringing litigation in California courts wherein it alleged that its principal place of business is located in San Jose, California.

21. As described infra, Yujun Wu, Qbit's principal, resides in California and maintains continuous business ties to the state. Wu holds a California driver's license, has registered and or maintains multiple businesses in California, and lists a California residence on his business registration documents.

22. As described infra, Yujun Wu and Qbit, through Bytechip, have operated in California and facilitated fraudulent cryptocurrency transactions. This involvement is evidenced by the US Department of Justice's forfeiture case filed in January 2024 —*USA v. All Funds Deposited, Credited, or Held*—where Bytechip's funds were frozen for suspected involvement in cryptocurrency and pig butchering related laundering and which resulted in the forfeiture of $1,215,221.99 (the "Bytechip Forfeiture Action").

23. Qbit's fraudulent business activities were intentionally directed at U.S. financial institutions and victims, including those in California, creating a substantial connection between Qbit and this forum.

24. Exercising jurisdiction over Qbit is reasonable and fair, as Qbit, through Bytechip and Wu, has long benefited from conducting business in California while simultaneously seeking to evade liability through improper corporate structuring.

25. Further, Defendants designed, contrived and effectuated the scheme set out herein from the State of California.

26. This Court has subject matter jurisdiction over this entire action pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d), because this is a class action in which the amount in controversy exceeds $5,000,000, exclusive of interest and costs, and any member of the Class is a citizen of state different from any defendant. Plaintiff is a citizen of Alabama and Wu is a citizen of California.

27. This Court has supplemental jurisdiction over the state law claims in this action pursuant to 28 U.S.C. § 1367, because the state law claims form part of the same case or controversy as those that give rise to the federal claims.

28. Venue is proper in this District because Defendant Qbit maintains an office in San Mateo, California and Defendant Wu maintains a residence and conducts business from Mountain View, California.

29. Assignment of this case to the San Jose Division is proper pursuant to Civil Local Rule 3-2(e) because a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in Santa Clara County, California.

III. PARTIES

30. Plaintiff Michael Mashkevich is an individual who currently and at all relevant times herein resides in the city of Albertville, Alabama.

31. Defendant Qbit is a Lithuanian Limited Liability Company, registration code 305577101. A true and correct copy of its company records are attached as Exhibit C and incorporated herein. Qbit's company records list Yujun Wu as the "head (director) of the company." (See, e.g., Exhibit C, UAB "Qbit Financial Service" Memorandum of Association, ¶ 7.6) Qbit has offices in the cities of Hangzhou and Shenzhen and in the special administrative region of Hong Kong. The primary location listed on Qbit's LinkedIn is No. 998 Canton Road, Kowloon Unit A2, 5/F, OfficePlus@Mong Kok, Kowloon, HK. (See https://www.LinkedIn.com/company/qbitneobank, last accessed Jan. 27, 2025.) Its website, Qbitnetwork.com, also lists a United States office at "Zanker Rd. Ste 110, San Jose, CA 95131." Qbit's counsel provided this website in a November 7, 2024 letter, attached hereto as Exhibit D and incorporated by reference. A copy of the relevant webpage, obtained from https://qbitnetwork.com/contact-us, is attached hereto as Exhibit E and incorporated by reference.

32. Qbit claims to be a legitimate banking-as-a-service company and owns the THGTen Destination Wallet. Qbit contends its services include "multi-currency business accounts, global payment processing, and supply chain financing." Its customers "may fund their accounts by transferring cryptocurrency, after which they can direct Qbit to use the deposited funds for payment purposes." (Exhibit D, ¶ 2).

33. Defendant Bytechip is a Delaware limited liability company registered to do business in California. Yujun Wu is listed as the chief executive officer and sole manager or member of Bytechip in the company's latest Statement of Information filed in California, dated July 24, 2024, which is attached as Exhibit F.

34. Defendant Wu is Qbit's incorporator and director. (Exhibit C, Memorandum of Association at ¶¶ 1.1, 7.6). At the time of Qbit's incorporation, Wu owned all shares of Qbit. (*id.*at ¶ 1.1). Wu was born in the People's Republic of China, from where he holds a passport, number ending in 5532. (*id* at ¶5.1). According to the complaint in the Bytechip Forfeiture Action, Wu also holds a California driver's license, number ending in 8032. A true and correct copy of the complaint in the

Bytechip Forfeiture Action — *United States of America v. All Funds Deposited, Credited, or held up to up to $2,029,765.39 in Solidfi vAccount # 9540002258156272 in the name of Gatcha Pictures LLC, beneficial owner Xuan Du; and, All funds deposited, credited, or held up to $2,979,690.04 in Solidfi v Account # 9540002258311162 in the name of Bytechip LLC, beneficial owner Yujun Wu*, U.S. District Court, Western District of Tennessee (Memphis), Case No. 2:24-CV-02036, filed Jan. 22, 2024—is attached hereto as Exhibit G.

35. Yujun Wu also goes by "Michael Wu." He uses these two names interchangeably, professionally and personally. For example, as a speaker at ZhenFund's "Looking Up | ZhenCraft·Overseas Adventurers" event, Wu was listed as "Wu Yujun" and introduced himself as "Michael Wu". A copy of the relevant webpage, obtained from https://en.zhenfund.com/News/51, is attached hereto as Exhibit H.

IV. PROCEDURAL HISTORY OF THE ALABAMA ACTION

36. On June 4, 2024, Plaintiff filed an original action in the Alabama Court against Ava, Miller, and Lee. A true and correct copy of the complaint is attached hereto as Exhibit I. He pled a cause of action for conversion and a request for injunctive relief. He simultaneously filed an emergency motion for a temporary restraining order and for an order to show cause why a preliminary injunction should not issue. That same day, the Alabama Court granted Plaintiff's motion, freezing the Destination Wallets (including THGTen) and scheduling the preliminary injunction hearing for June 14, 2024.

37. On June 14, 2024, the Alabama Court issued a Preliminary Injunction Order, enjoining Ava, Miller, Lee and the non-party exchanges at which Plaintiff's stolen funds were held from "withdrawing, transferring, selling, encumbering, or otherwise altering any of the cryptocurrency or assets held in the wallet addresses" listed in Appendix B. No defendants appeared at the hearing to contest the injunction.

38. Approximately seven months later, on January 20, 2025, Qbit filed a motion seeking to dissolve the injunction. A hearing for the motion was set for February 7, 2025. A true and correct copy of Qbit's motion is attached here as Exhibit J.

39. On February 4, 2025, Plaintiff filed in the Alabama Court an Omnibus Motion to Strike Yujun Wu's Declaration and Response to Qbit's Motion to Dissolve (attached as Exhibit K) with an evidentiary submission; a Motion to Continue the February 7 Hearing (attached as Exhibit L); and a Notice to Serve a Third-Party Subpoena on Qbit. Qbit filed a response to the Motion to Continue the same day.

40. The hearing on Qbit's motion occurred on Friday, February 14, 2025. The Alabama Court has not ruled on Qbit's motion but may any day. None of Qbit, Bytechip, or Yujun Wu are parties in that case.

V. DEFINITIONS AND BACKGROUND ON CRYPTOCURRENCY

41. "**Virtual currencies**," also known as cryptocurrency, are digital tokens of value circulated over the Internet as substitutes for traditional fiat currency. Virtual currencies are not issued by any government or bank, like traditional fiat currencies such as the U.S. dollar, but are generated and controlled through computer software. Bitcoin ("BTC") and Ethereum ("ETH") are the most well-known virtual currencies in use.

42. Virtual currency addresses are the virtual locations to which such currencies are sent and received. A virtual currency address is analogous to a bank account number and is represented as a string of alphanumeric characters. Like with bank accounts, you cannot send money to a virtual address without knowing the specific string of characters. Typically, someone will only send money to an address if know the owner and the owner shares their unique address with the sender.

43. The identity of an address owner is generally anonymous (unless the owner opts to make the information publicly available), but analysis of the blockchain can sometimes be used to identify the owner of a particular address. The analysis can also, in some instances, reveal additional addresses controlled by the same individual or entity. Each virtual currency address is controlled using a unique corresponding private key, a cryptographic equivalent of a password needed to access the address. Only the holder of an address's private key can authorize a transfer of virtual currency from that address to another address. A user of virtual currency can utilize multiple addresses at any given time and there is no limit to the number of addresses any one user can utilize.

44. "**Blockchain**" is used by many virtual currencies to publicly record all of their transactions. The blockchain is essentially a distributed public ledger, run by a decentralized network of computers, containing an immutable and historical record of every transaction that has ever occurred utilizing that blockchain's specific technology. The blockchain can be updated multiple times per hour and record every virtual currency address that ever received that virtual currency. It also maintains records of every transaction and all the known balances for each virtual currency address. There are different blockchains for different types of virtual currencies.

45. "**Virtual currency wallet**" is a software application that interfaces with the virtual currency's specific blockchain and generates and stores a user's addresses and private keys. A virtual currency wallet also allows users to send and receive virtual currencies. Multiple addresses can be stored in a wallet.

46. "**Stablecoin**" is a digital asset that is designed to maintain a stable price over time. They are often pegged to a fiat currency, like the U.S. dollar, and maintain a 1:1 ratio with it, and backed by collateral. Stablecoins can be used to hold money within the crypto ecosystem. USD Coin ("USDC") is a type of fiat-backed stablecoin. It is tied to the value of the U.S. dollar; therefore, one unit of USDC is equivalent to approximately one U.S. dollar.

47. **"Centralized Exchanges**" allow owners of digital assets trade their cryptocurrency. OKX, for example (available at okx.com and corresponding apps) operates like other financial services platforms – Schwab, Morgan Stanley, and others. It holds billions of dollars' worth of crypto and requires users to comply with Know-Your-Customer (KYC) and Anti-Money-Laundering (AML) procedures to ensure regulatory compliance and discourage illicit activities. Users download the app or register on the website, deposit their funds, and invest. Because OKX is a legitimate, trustworthy exchange, the user would be able to withdraw or transfer funds from such an account freely.

48. A substantial market for fraud has grown secondary to the legitimate platforms. Phony exchanges promising outrageous returns to have been established and continue to operate with the sole purpose of conning unsuspecting people out of their entire life savings. The FBI estimates such sites have been used to steal billions of dollars.

VI. THE INTERNATIONAL PIG BUTCHERING CRISIS (A BRIEF OVERVIEW)

49. Mr. Mashkevich and the Class had their cryptocurrency stolen as part of elaborate pig butchering scams. According to the FBI, pig butchering scams cost Americans $5.3 billion in 2023 alone, with 40,000 U.S. victims reporting the scams to law enforcement. Various sources estimate that only 15% - 25% of U.S. pig butchering victims report the crimes, meaning the U.S. likely had a minimum of 160,000 pig butchering victims in 2024, scamming unwitting victims–like Plaintiff and the Class–out of an estimated $20 billion annually.

A. How Pig Butchering Works

50. Pig butchering scammers conduct an elaborate, long-term psychological attack on their victims with the intent of stealing victims' cryptocurrency through deception. The scammers contact potential victims through social media, dating apps, direct messaging platforms, or text. As just one initial contact example, the potential victims may receive a text from an unknown number that simply says "hello." The scammers are seeking any response, such as the potential victims replying to ask who sent the text. From there, the scammers seek to build personal relationships with the targets, manipulating them into believing the scammers are potential romantic interests or trusted friends.

51. After the scammers establish trust, they introduce the victim to the idea of investing in or with cryptocurrency or by earning cryptocurrency by doing online work from home. The scammers guide the victims to a fake cryptocurrency trading platform. These websites look legitimate, with polished interfaces and simulated trading data, and the scammers convince the victims that the victims are controlling their own invested cryptocurrency.

52. After the victims have invested a large sum, the scammers make it impossible for the victims to withdraw their funds. If the scammers believe the victims can be tricked further, explanations may follow to convince the victims to invest even more crypto. For example:

- The scammers may tell the victims their accounts have been so profitable that the IRS requires the victims to pay capital gains tax in advance.
- As was the case with Mr. Mashkevich, the scammers identify alleged technical issues or processing fees the victims need to pay before the victims' accounts are unfrozen.

53. At some point, the platform itself will disappear, or the scammer will block the victim. The victims then realize they have been scammed, but their cryptocurrency is gone. The cryptocurrency can then only be retrieved with blockchain analysis and court-ordered wallet freezes to stop the process of cryptocurrency laundering before the cryptocurrency is taken off the blockchain and converted to fiat currency, at which point it is unreachable.

B. The Second Layer of Pig Butchering Victims

54. Pig butchering scams create financial tragedy for the scam victims, but the international criminal operation is fueled by a second layer of tragedy - the scammers themselves are often victims of human trafficking. Trafficking victims are lured with promises of legitimate jobs, such as customer service or IT work. During their recruitment, the traffickers target vulnerable populations, particularly in Southeast Asia, China, and Africa. Once the victims arrive at the scam compounds, their passports and phones are confiscated, and they are forced to work in pig butchering and other scam operations.

55. For example, a Vietnamese teenager named Nguyen Thien Kai moved to Cambodia after she was promised a high salary for teaching people how to play online games. But once she crossed the border, she was sent into a basement and instructed to scam people. The 19-year-old realized she had been tricked. "I had hidden my phone and managed to text my family to let them know what happened. But then the boss saw my phone and took it," she said. "He read the texts to my family telling them to call the police, and he beat me and sold me to another organization."[4]

56. Former prosecutor Erin West summarized the human trafficking tragedy fueling pig butchering scams during an interview with Ali Rogan of PBS News:

> We have literally never seen a world crisis like this. We've got Americans and people all over the world who've lost all their money. . . . [W]e have human trafficked victims that are forced to do this dirty work . . . . And when they get there, their passports are seized, they're put in buses and they are moved to these compounds where they are surrounded with men with AK47s . . . . The NGOs that I spoke with on the ground in Southeast Asia told me 7 out of 10 women are coming out of there saying that they

[4] https://www.abc.net.au/news/2022-09-16/cambodia-human-trafficking-online-scam-pig-butchering/101407862

were sexually assaulted . . . . 300,000 [people] estimated by the United States Institute of Peace are behind held against their will.[5]

C. The Criminal Masterminds Behind Pig Butchering

57. The international crime syndicates operating these scams include but are not limited to the Chinese 14K Triad and the Karen Border Guard Force. Wan Kuok-Koi a/k/a "Broken Tooth" is a reputed Chinese mafia boss who has been sanctioned by the U.S. Government. He is the former head of the Chinese 14K Triad.[6] The 14K Triad is a criminal operation based in Hong Kong with ties to various scam compounds, such as KK Park, an online scam factory on Myanmar's border with Thailand.[7]

KK Park, a scam factory on Myanmar's border with Thailand, where several of the human trafficking victims repatriated on February 29, 2024 were held. captiveImage: Stefan Czimmek/DW

58. In 2018, "Broken Tooth" established the World Hongmen History and Culture Association in Cambodia, which reflects a criminal co-opting of the name of a centuries old Chinese fraternal organization first established in the mid-1600s. Broken Tooth also heads the Dongmei Group based in Hong Kong, which invests in the Saixigang Industrial Zone in Burma (Myanmar).[8] The Saixigang Zone, along with Myanmar's KK Park (pictured above) and other scam compounds, houses industrial-scale cyberfraud operations, engages in human trafficking, and has "clear links to organize

[5] https://www.pbs.org/newshour/show/how-human-trafficking-victims-are-forced-to-run-pig-butchering-investment-scams

[6] https://www.wsj.com/world/china/china-mafia-broken-tooth-wan-kuok-koi-online-fraud-scam-70c09afb

[7] https://www.dw.com/en/china-repatriates-hundreds-of-scam-factory-survivors/a-68408165

[8] https://kh.usembassy.gov/treasury-sanctions-corrupt-actors-in-africa-and-asia/

crime figureheads Wan (Broken Tooth) Kuok Koi and She Zhijiang."[9] Notably, Myanmar is one of only three countries on the FATF money laundering and terrorist financing black list, along with North Korea and Iran.[10,11]

59. The Karen Border Guard Force (KBGF) is a violent militia that controls much of Myanmar's border areas with China, Laos, and Thailand. The KBGF operates in Myanmar's Karen State and is headed by Colonel San Myint a/k/a Saw Chit Thu. The KBGF has overseen the development of numerous illegal casino operations, which are used as pig butchering scam compounds. The KGBF changed its name in 2024 to the Karen National Army (KNA). The KBGF/KNA is considered a "major node in a network of cyber scam centers . . . in Southeast Asia in which criminal groups are earning billions of dollars."[12]

60. The KGBF/KNA partnered with the Hong-Kong registered Yatai International Holdings Group to generate revenue through companies forced to leave China because of it's crackdown on illegal casino operations.[13] "Myanmar has become the prime destination for criminal groups", where money laundering and online scam operations relocated after several governments in southeast Asia cracked down on criminal gangs.[14] While an exhaustive discussion of the international criminal gangs perpetrating pig butchering scams is beyond the scope of this filing, the Court's awareness of the global criminal enterprises perpetrating the scam at issue in this case is important for the Court's determination as to appropriate next steps in this litigation.

---

[9] https://www.unodc.org/roseap/uploads/documents/Publications/2024/Casino_Underground_Banking_Report_2024.pdf

[10] https://www.fatf-gafi.org/en/countries/black-and-grey-lists.html.

[11] The FATF is the Financial Action Task Force, an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering and terrorist financing. The FATF blacklist identifies high-risk jurisdictions subject to a call for action because of their known close association with money laundering and terrorist financing. *See* FN7, *supra*

[12] https://www.justiceformyanmar.org/stories/the-karen-border-guard-force-karen-national-army-criminal-business-network-exposed

[13] https://www.usip.org/publications/2020/04/chinese-crime-networks-partner-myanmar-armed-groups

[14] https://www.usip.org/publications/2025/01/how-crime-southeast-asia-fits-chinas-global-security-initiative

D. Off-Ramping – From Stolen Cryptocurrency to Fiat Currency

61. The goal of the international crime syndicates perpetrating pig butchering cryptocurrency scams is to off-ramp the cryptocurrency by moving assets on a blockchain such as Tether or Tron and ultimately off chain to fiat currency. If the stolen crypto is on the blockchain, there is a chance it can be tracked and frozen. Once the cryptocurrency is off-ramped—for example if the stolen cryptocurrency frozen in the Qbit cyberwallet is released so that it can be off-ramped and converted to fiat currency—pig butchering victims have no realistic path to recovery. To accomplish the off-ramping, criminals will send cryptocurrency to a digital wallet and instruct the wallet owner to move the cryptocurrency to other wallets as part of the laundering process or ultimately accounts held at centralized exchanges, where it can be converted into fiat currency.

62. Laundering large amounts of cryptocurrency requires sophisticated techniques. Money laundering traditionally involves three stages – placement, layering, and integration. Placement is the process of moving the funds away from a direct association with the crime. With cryptocurrency, placement is the movement of cryptocurrency out of the Deposit Wallets into which the victims unwittingly transferred their cryptocurrency. Layering seeks to move the funds in a complex pattern to disguise the trail of funds and frustrate attempts to track the stolen funds. With cryptocurrency, layering involves numerous transactions along the blockchain to disguise where the funds went. Integration is the process of making the stolen funds available to the criminals who stole the funds after the funds have been "washed".[15]

63. As part of the laundering process, cyber criminals deploy various techniques. such as:

- Exchange hopping - using multiple crypto exchanges to transfer funds across different platforms
- Staggering –structuring transfers in a way that reduces detection risk by dispersing funds across multiple transactions, wallets, or time intervals
- Mixing or Commingling- blending crypto from multiple sources to obscure the transaction history. Digital banks that offer banking-as-a-service (BaaS) in jurisdictions deficient in their anti-money laundering systems afford criminals the opportunity to "cloak" the stolen crypto by mixing it with legitimate funds

[15] https://www.unodc.org/unodc/en/money-laundering/overview.html

VII. THE SCHEME

A. The Class Is Pig Butchered

64. Defendants and their co-conspirators followed an especially pernicious version of the "pig butchering" roadmap for cryptocurrency theft. Promised significant gains in return, Class Members were enticed to spend time performing online tasks or investing cryptocurrency. Regardless of whether the scheme presented to a scam victim involves work from home or investments, the Scammers' playbook and methods are consistent across the Class, reflecting a methodologically and psychologically sophisticated approach of manipulation and theft. Throughout, Class Members were promised and believed they could withdraw the money they had earned. In reality, they were coerced to make additional payments before withdrawing their money, money that would never be returned and had already been stolen.

65. After making initial contact with victims, the Scammers "train" the target to use online platforms to complete the necessary tasks or make the recommended investments. Here, the Scammers "trained" Plaintiff, who then began performing what Plaintiff thought were tasks associated with optimizing applications for two legitimate companies, Grayphite and Resy. In truth, Plaintiff was unknowingly interacting with sham websites designed by the Scammers to further their theft scheme. This is a technique consistent across the Class.

66. Plaintiff was contacted by the Lee on or about March 20, 2024, regarding supposed part-time online work related to Grayphite. Their initial conversation is reproduced in the Alabama Complaint (Exhibit I, ¶ 26). On March 29, 2024, Plaintiff sent an initial deposit of $110 of USDC, a cryptocurrency, from his Coinbase account to an account that the Scammers represented was part of the work platform. Plaintiff subsequently performed tasks on this fake work platform and received "payments," evidenced in his growing account balance.

67. On April 6, 2024, the Scammers, through Miller, contacted Plaintiff about an additional related job opportunity that involved similar online work for another legitimate company, Resy. Their initial conversation is reproduced in the Alabama Complaint (Exhibit I, ¶ 27). On April 7, 2024, Plaintiff began making additional deposits from his Kraken[16] account related to this job

[16] Kraken is a widely used and legitimate cryptocurrency investment platform.

opportunity, beginning with a $10 deposit and progressively increasing. As with Plaintiff's Coinbase deposits, The Scammers permitted Plaintiff to withdraw small amounts of money he had "earned" and deposit those funds to his Kraken account, but Plaintiff was required to replenish funds to earn additional amounts.

68. During April 2024, Plaintiff made progressively increasing deposits and withdrawals. The Scammers enticed and coerced these deposits through a variety of standardized methods, including: 1. Fake account balances on the online cryptocurrency wallet balances through the fake online work platforms that purportedly reflected Plaintiff's monetary balance in the systems; 2. Allowing Plaintiff to withdraw small amounts of cryptocurrency 'from' the platform to his personal cryptocurrency wallet to advance the illusion that he was performing real work; 3. Representing that Plaintiff could make increasing commissions if he deposited increasing amounts; and 4. Saddling his account with hidden fees or deposits that he was required to pay before he could complete tasks or withdraw money.

69. For example, after Lee and Miller separately persuaded Plaintiff that he could withdraw his cryptocurrency at any time, Plaintiff began encountering so-called "combination tasks" on the platforms. These "combination tasks" caused Plaintiff's balance to appear negative, and Lee and Miller convinced Plaintiff that he needed to transfer greater amounts of cryptocurrency into the system to "free up" his account and enable him to earn higher commissions from performing combination tasks.

70. Similarly, the Scammers employed a fake "credit score" to persuade a target to deposit additional funds. When Plaintiff tried to withdraw funds from the sham Grayphite platform but was unable to do so, he reached out to Lee on WhatsApp. Lee told Plaintiff his "credit score" on the platform had dropped to 80%, and he needed to restore his score to access his cryptocurrency. Plaintiff that had two options to restore his credit score. Option 1 was to pay $20,000 ($1,000 per point to restore) and reset his credit score immediately. Option 2 was he could wait 10 months for his score to return to 100%. To induce Plaintiff's further deposits, Lee offered to help financially with Option 1.

71. The Scammers also told Plaintiff on April 17, 2024 that he could not withdraw his commissions because he owed "taxes" on them. Lee once again offered to assist Plaintiff, this time by supposedly transferring cryptocurrency into Plaintiff's account. The Scammers' theft scheme involved threats related to alleged law enforcement involvement. On April 19, 2024, Lee contacted Plaintiff via WhatsApp to convince him that the FBI was involved, claiming that Lee had unwittingly "helped" Plaintiff with stolen funds that Lee had borrowed from a friend. These tactics are all part of the standardized playbook used by the Scammers to ensnare Plaintiff and the Class Members.

72. In sum, the Scammers used a systematic multi-stage scheme to target Class Members, including Plaintiff, and lured them to transfer increasing amounts of cryptocurrency to the Deposit Wallets as part of fake work or investment platforms. In aggregate, Plaintiff transferred approximately $90,000 to Deposit Wallets controlled by the Scammers and their co-conspirators. A more detailed accounting of the timeline and Scammers' tactics is available in the Alabama complaint attached hereto as Exhibit I.

73. The final step in this scheme, as described below, involved the Laundering Network and was identical for all Class Members: Defendants or their co-conspirators stole the funds, transferred the stolen cryptocurrency from the Deposit Wallets to one or more of the thirteen Pivot Wallets, and then embarked upon the process of laundering the stolen cryptocurrency to the Destination Wallets for eventual off-ramping of the stolen cryptocurrency by converting it to fiat currency.

74. To trace the stolen cryptocurrency, Plaintiff employed Inca Digital ("Inca"), a cryptocurrency investigation firm. Inca's investigation revealed that the Scammers converted Class Members' assets, including Plaintiff's assets, and then sent those assets through a web of transactions designed to hide their trail. Inca traced and connected the Scammers' and Defendants' trail of transactions and identified the cryptocurrency wallets that held Class Members' funds.

75. Inca's investigation was conducted in two phases, both employing rigorous blockchain forensic techniques. In phase one, Inca performed a "forward trace," tracking the flow of Plaintiff's funds from their initial transfer to intermediary wallets and eventually to end-point wallets hosted on

exchanges and third-party platforms, including to some of the Destination Wallets listed in Appendix B.

76. In phase two, Inca "reverse traced" the flow of funds from the initial, intermediary, and end-point wallets identified in phase one and determined that additional addresses matched Plaintiff's flow of funds through the Laundering Network as part of a common scheme involving other Class Members. Through this tracing, Inca was able to confirm the identity of wallets involved in cryptocurrency transactions that were part of the common scheme, including the identity of the Destination Wallets, which ultimately received Class Member funds and accordingly should remain frozen. Those wallets are set forth in Appendix B, categorized by exchange.

77. The bottom line of Inca's analysis is that Class Members' funds were initially deposited into the Deposit Wallets listed in Appendix A and were ultimately sent to the Destination Wallets listed in Appendix B. It is the Destination Wallets listed in Appendix B that Plaintiff sought to, and which the Alabama Court did, freeze in its June 4, 2024 Order for Temporary Restraining Order and to Show Cause and its June 14, 2024 Preliminary Injunction Order.

78. Qbit claimed ownership of one of the wallets included in Appendix B, OKX Destination Address THGTen. At least $1 million and potentially millions more are traceable to Qbit's THGTen Destination Wallet.

79. Freezing the funds in the Destination Wallets is the only realistic way of obtaining recovery for the victims of the Scammers' scheme, including Plaintiff and the Class.

B. Flow of Victim Funds to Qbit's THGTen Destination Wallet

1. <u>Transactions Originating on the Ethereum Blockchain</u>

<u>Part 1: Victims Send Ethereum to the Scammers, Who Convert the Stolen Funds to USDT and Transfer Them to the Tron Blockchain.</u>

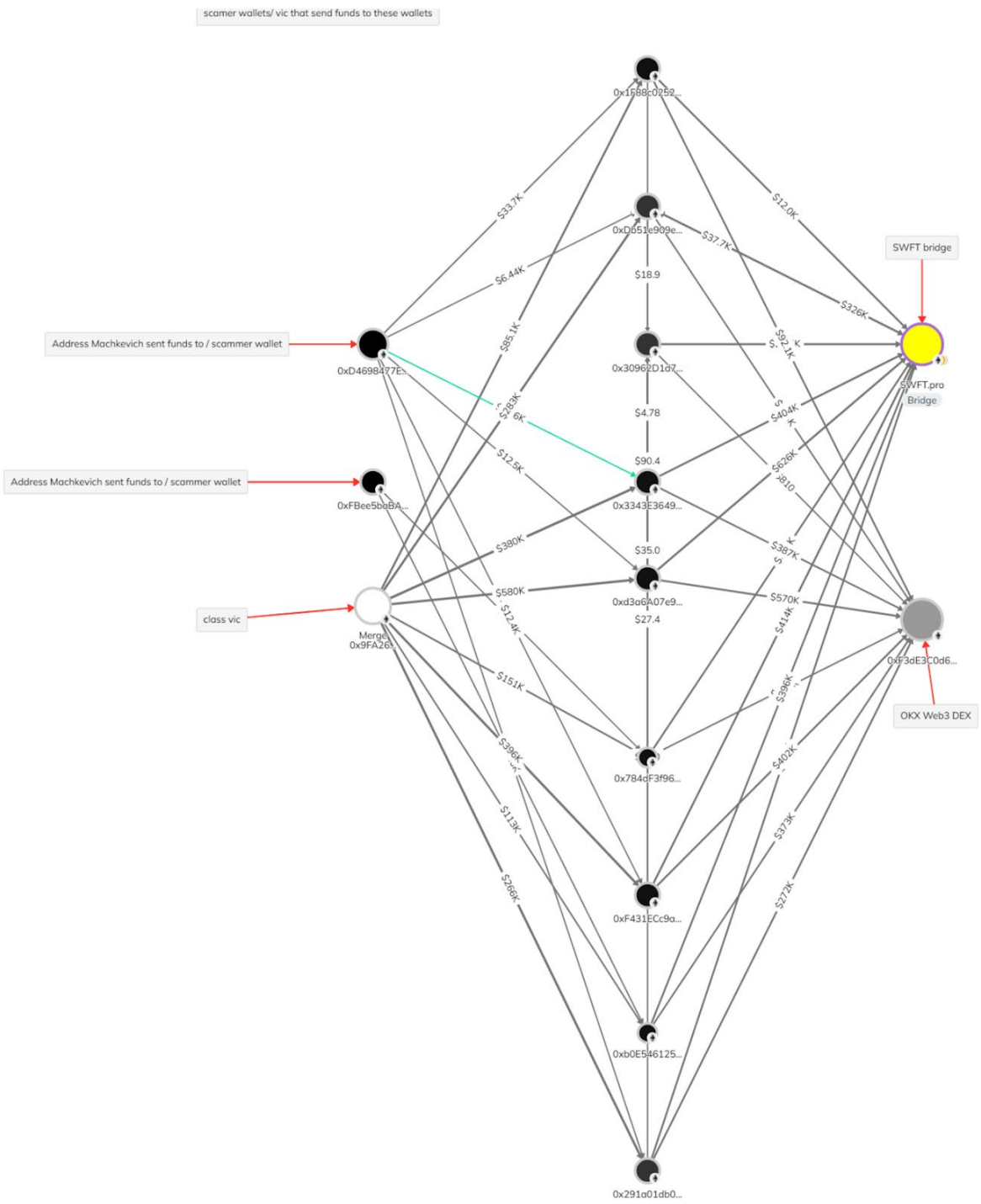
80. Plaintiff and other Class Members sent cryptocurrency to one or more of the Deposit Wallets, whose owners then sent the funds to the Pivot Wallets, converted them to USDT, and sent them to a Bridge address for transfer to the Tron blockchain.

Step 1.1: Victim Funds enter the scam network and are sent to pivot addresses

81. Plaintiff sent funds on the Ethereum blockchain to two Deposit Wallets (at addresses: 0xD4698477E65C7be219094aC71F65F40582EF5dbe and 0xFBee5baBA85C839e3E6aBD11b7eF4D8001357f82). These two Deposit Wallets, controlled by the Defendants or their co-conspirators, transferred the funds to eight different Pivot Wallets, listed in Appendix D. An additional 54 Deposit Wallets, included in Appendix A, sent stolen funds from hundreds of additional Class Members to the same Pivot Wallets.

Step 1.2: Victim Funds are Converted to USDT and Transferred to the Tron Blockchain

82. From the Pivot Wallets, Defendants or their co-conspirators sent the funds to the OKX Web3 DEX Router (0xF3dE3C0d654FDa23daD170f0f320a92172509127), where the ETH was converted to USDT. The converted funds were then sent back to the Pivot Wallets and transferred to the Tron blockchain via a SWFT Bridge (0x92e929d8B2c8430BcAF4cD87654789578BB2b786). The image below shows the Ethereum path from victims' addresses to the SWFT Bridge, read left to right.



83. From the SWFT Bridge, Defendants or their co-conspirators sent funds on the Tron blockchain to nine bridge destination addresses. Funds from three of the bridge destination addresses are traceable to Qbit's THGTen Destination Wallet: TUrhEAu6ufCvDtpKdDjJAZAGpNVDJoVVhg TDBzuM9hAvBHP6yae417es9oqK66NEqVJ7; and TCsAJrom3GBrtzToRgfi9rA5sA2cbbtqVB

Part 2: Victim Funds are Staggered and Commingled on the Tron Blockchain Before Consolidation at Qbit's "Cregis Wallet" and Transfer to THGTen.

84. From the three bridge destination addresses, Defendants or their co-conspirators sent Class Member funds through a series of intermediary wallets, where Defendants or their co-conspirators commingled Class funds with other sources before consolidating them at the Cregis Master Wallet.

Step 2.1: Defendants or their co-conspirators began staggering class funds—breaking transactions into smaller amounts to obscure the source of funds—before consolidating them at Culminating Point 1

85. First, Defendants or their co-conspirators sent at least $1,653,081 USD of traceable Class funds from the three bridge destination addresses, above, to TUAhG2WLLvmvtu6houNWmd4d6TK83d3Hbc (Culminating Point 1). Most funds flowed directly to Culminating Point 1, but some funds passed through intermediary hops.

Step 2.2: Defendants or their co-conspirators continue staggering class funds, before consolidating them at Culminating Point 2

86. Then, Defendants or their co-conspirators sent at least $1,653,081 USD of traceable Class funds from Culminating Point 1 to TNJbYSmWUGhQEv1AuVdLHHZNCHzEyS8VaC (Culminating Point 2). The funds passed through five intermediary hops before reaching Culminating Point 2.

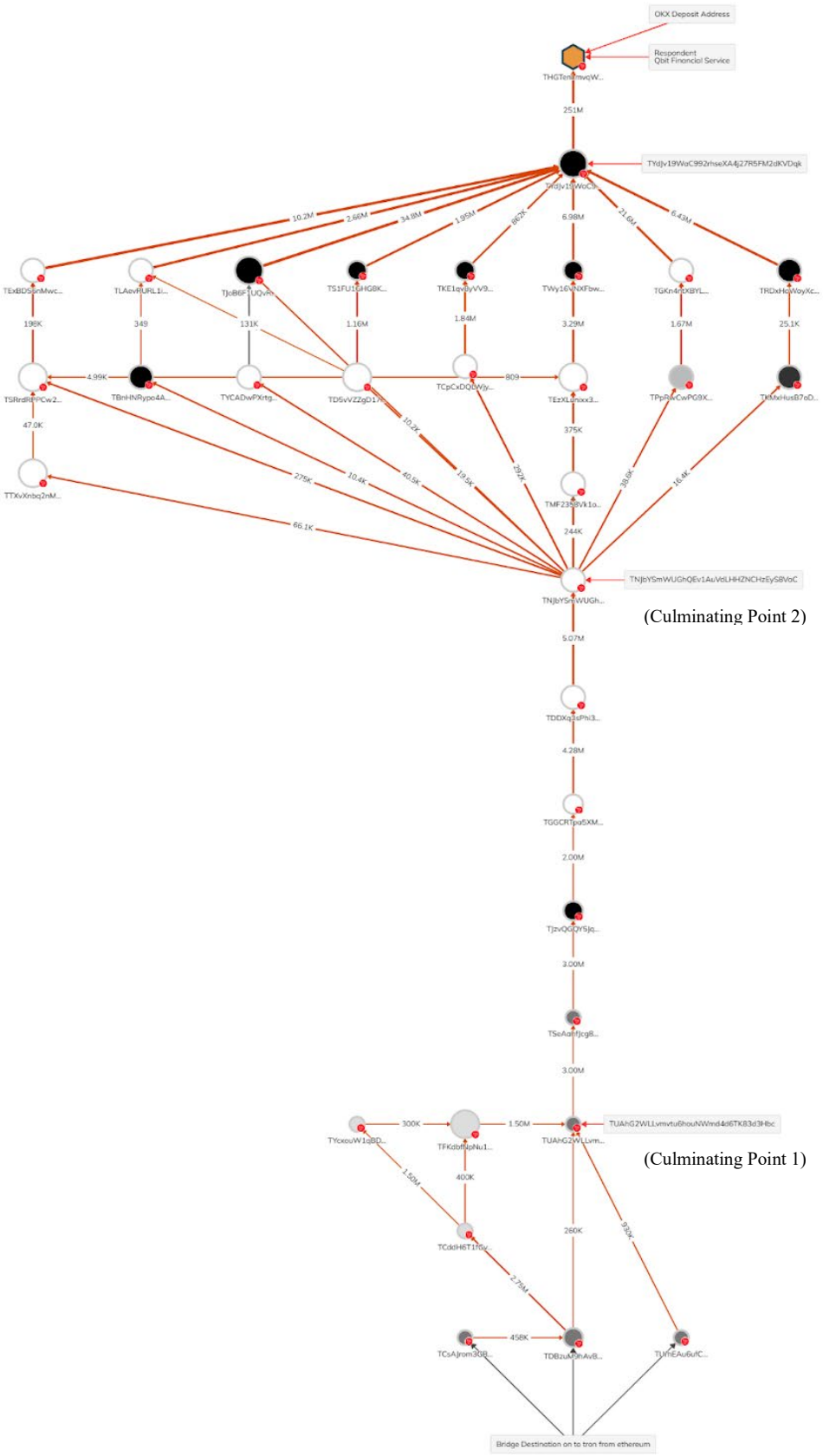
Step 2.3: Defendants or their co-conspirators further stagger class funds before Consolidating at Qbit's Cregis Master Wallet (Culminating Point 3)

87. From Culminating Point 2, Defendants or their co-conspirators broke the Class funds into smaller transactions and distributed them across a network of additional addresses. Defendants or their co-conspirators commingled class funds with other sources before consolidating and sending them to the Cregis Master Wallet. Ultimately, Defendants or their co-conspirators sent at least **$1,092,200** USD of traceable Class funds from Culminating Point 2 to the Cregis Master Wallet.

88. In their Nov. 7 letter, Qbit counsel indicated Qbit owned the Cregis Master Wallet, referring to it as the "Master Cregis Wallet".

Step 2.4: Consolidated Funds are Sent to Qbit's THGTen Destination Wallet

89. The Cregis Master Wallet serves as a staging area where previously fragmented funds are recombined. Once commingled and consolidated, Defendants transferred at least $1,092,200 of traceable Class funds into Qbit's THGTen Destination Wallet. The image on the next page shows the transaction path of class funds on the Tron blockchain, as described in Part 2, above.


OKX Deposit Address
Respondent
Qbit Financial Service
251M
6.98M
10.2M
2.66M
34.8M
1.99M
862K
21.6M
6.43M
198K
349
131K
1.16M
1.84M
3.29M
1.67M
25.1K
4.99K
809
47.0K
375K
275K
10.4K
40.5K
10.2K
19.5K
297K
39.6K
16.4K
66.1K
244K
(Culminating Point 2)
5.07M
4.28M
2.00M
3.00M
3.00M
300K
1.50M
1.50M
400K
260K
2.78M
458K
(Culminating Point 1)
Bridge Destination on to tron from ethereum

Additional Class Losses originating on the Polygon Chain.

90. Most Class losses did not originate on the Ethereum blockchain, as described above, but were instead sent from Class Member wallets to Deposit Wallets on the Polygon blockchain. These funds followed an analogous path to those on the Ethereum chain. First, Class Members sent USDC to the Deposit Wallets. Defendants or their co-conspirators then sent the Class Members' funds from the Deposit Wallets to the Pivot Wallets, and then from the Pivot Wallets to a Bitget Wallet Swap Bridge where they converted the funds to USDT and transferred them to the Tron blockchain. Once converted and transferred, Defendants or their co-conspirators again staggered and commingled the USDT to hide the source and impede recovery of the stolen funds. After passing them through a complex path of intermediary wallets, Defendants and their co-conspirators eventually consolidated the stolen funds at several Destination Wallets, including those listed in Appendix B.

91. Altogether, at least an estimated $25 million of additional Class losses were sent from Class Members' wallets on the Polygon chain into the Laundering Network. Some of the funds originating on the Polygon chain also entered the same Tron pathway to Qbit's THGTen Destination Wallet, with an additional estimated $1.5 million class funds traceable to Culminating Point 1.

92. Across both the Ethereum and Polygon blockchains, Defendants and their co-conspirators converted at least an estimated $28 million of Class Member funds. At least $1 million of these funds are traceable to Qbit's THGTen Destination Wallet.

C. Qbit's Omissions and Misrepresentations in the Alabama Action

93. On June 4, 2024, Plaintiff filed an action in the Alabama Court against Ava, Miller, and Lee. He simultaneously filed an emergency motion for a temporary restraining order and for an order to show cause why a preliminary injunction should not issue, which the Court granted that same day. On June 14, 2024, the Alabama Court issued a Preliminary Injunction Order, enjoining Ava, Miller, Lee and the non-party exchanges at which Plaintiff's stolen funds were held from "withdrawing, transferring, selling, encumbering, or otherwise altering any of the cryptocurrency or assets held in the wallet addresses" listed in Appendix B.

94. On January 20, 2025, Qbit filed in the Alabama Court a Motion to Dissolve or Modify the Court's June 14, 2024, Order granting a Preliminary Injunction, over seven months after the

Alabama Court entered its order. Qbit relied on a declaration from Qbit CEO Yujun Wu. Throughout the pleading, Qbit attempted to legitimize its operations while misleading the Court by both omission and affirmative misrepresentation and failed to substantiate any of its claims. Among Qbit and Wu's vague and unsupported claims, they asserted:

95. **First**, that Plaintiff "demanded" a "Ransom Payment" from Plaintiff's Hong Kong counsel. (Exhibit J, Motion at pp. 11 – 12). This "ransom payment" was actually a settlement offer, made at the request of Qbit's Hong Kong counsel.

96. **Second**, that "[t]he Qbit Wallet contains approximately $7 million worth of cryptocurrency" and that "[b]ecause the Injunction Order froze the Qbit Wallet," Qbit "must borrow money at high interest rates to pay back funds to its customers," causing it to lose $6,000 each day. (*Id.*, Motion at p. 12; Exhibit A at ¶¶ 7-8). Despite claiming to be losing $6,000 per day, Qbit and Wu waited seven months before filings their Motion to Dissolve. Defendants offered no proof that Qbit borrowed to repay funds to its customers. They did not identify the lenders, the amounts, the fiat currency, the dates, the interest rates, or the amortization schedules for the alleged loans.

97. **Third**, that the $7 million in the THGTen Destination Wallet was "all deposited by Interlace account holders that have been screened through Interlace's quality assurance procedures." (*Id.*, Motion at p. 12; Exhibit A at ¶ 7). While clearly implying that Interlace's "quality assurance procedures" establish the stolen cryptocurrency was obtained by honest means, they offer no information about Interlace other than to claim Interlace "is only open to registered business and may be used for business purposes only" and to briefly describe the "various certifications and business documents" Interlace customers must provide to register. (*Id.*, Motion at pp. 4-5; Exhibit A at ¶ 4)

98. Despite their reliance on Interlace to bolster their credibility and assuage concerns of money laundering, they failed to disclose that Interlace is deeply intertwined with Qbit, including that they share significant digital infrastructure and the same founder and CEO, Defendant Wu.

99. This common digital infrastructure is highly indicative of close operations ties and is evident from an analysis of each companies' HTML source code and of IP Address 47.89.250.82. The HTML Source code on both sites contain an identical warning: "We're sorry but **QbitPay** doesn't work properly without JavaScript enabled. Please enable it to continue." (Emphasis added). Both websites

also use the same website analytics library (NPSMeter), and the NPSMeter integration on both sites uses the same account identifier (9698c2ea853caafe).[17] Finally, the computer infrastructure at IP address 47.89.250.82 has domain name resolutions to qbitnetwork.com, ipeakoin.com,[18] and interlace.money.[19]

100. Moreover, Wu is the CEO and founder of Interlace, just as he is the CEO and founder of Qbit. On his LinkedIn page, Wu claims to have been the Interlace CEO since 2021. Interlace's LinkedIn lists Michael Wu as its CEO and founder.[20] But in his Declaration, Mr. Wu does not acknowledge that he is the CEO of Interlace. Instead, he uses vague assertions regarding Qbit's use of the Interlace platform, concealing the fact that Interlace is his company, not an independent third party.

101. **Fourth**, that Qbit's customers "may fund their accounts by transferring cryptocurrency" and "direct Qbit to use the deposited funds for payment purposes" and that Qbit uses OKX "to provide trading services related to it[sic] virtual assets." (*Id.*, Motion at pp. 4, 5; Exhibit A at ¶¶ 3, 5). An analysis of their cryptocurrency wallet, the THGTen Destination Wallet, shows that the wallet received $250 million in USDT between March 5 and June 6, 2024. In that same three-month period, Qbit purportedly transferred all but $7 million from the THGTen Destination Wallet, draining the wallet of over 97% its funds. Despite Qbit's claim that it uses its OKX accounts for clients' "payment purposes" and "to provide trading services," the wallet averaged only 1.66 transfers per day, suggesting that the account is not actively engaged in transactional activity.

---

[17] Companies typically include website analytics libraries to track visits to their website and users' experience when browsing the site. To differentiate between different customers' data, a website analytics library like NPS Meter will give each customer a unique identifier to compartmentalize customer integrations.

[18] Interlace was founded as iPeakoin in 2019 and announced its rebrand to Interlace on August 20, 2024.

[19] A domain name can be thought of as a shortcut directly from your browser to the proper server, represented by the IP address

[20] Interlace, LinkedIn Profile, https://sg.LinkedIn.com/company/interlace-money?trk=public_post_feed-actor-name (last accessed Jan. 27, 2025); *see also* Interlace, LinkedIn Post, https://www.LinkedIn.com/posts/interlace-money_weareinterlace-interlace-interlacemoney-activity-7265659464840 560640-

D. Qbit, Yujun Wu, Interlace, and the Intersection of Criminal Conduct, Fintech, and BaaS

1. Qbit – Scope of Business

102. Qbit holds itself out as a legitimate BaaS company and claims ownership of the THGTen Destination Wallet. Qbit contends its services include "multi-currency business accounts, global payment processing, and supply chain financing." Its customers "may fund their accounts by transferring cryptocurrency, after which they can direct Qbit to use the deposited funds for payment purposes." (Exhibits D and J).

2. Qbit's Functional Alter Ego Bytechip LLC

103. Defendant Bytechip is a limited liability company registered in both Delaware and California. It is registered as Delaware file number 736317 and California file number 202021210840. On July 30, 2020, Yujun Wu filed an "Application to Register a Foreign Limited Liability Company" with the California Secretary of State to register Bytechip in California. True and correct copies of Bytechip's State of Delaware Limited Liability Company Certificate of Formation and California Secretary of State Application to Register a Foreign Limited Liability Company are attached as Exhibits M and N, respectively.

104. Qbit formerly operated as Bytechip. Defendant Bytechip did business as Qbit, was owned by Qbit's executive officer, Yujun Wu, and had an office at the same address as Qbit: 2381 Zanker Rd, Ste 110, San Jose CA 95131. Defendant Bytechip's operation under the name Qbit is identified in two different federal court cases. In *Bytechip, LLC v. Solid Financial Technologies, Inc. et al*, Bytechip identifies itself in the caption as "Bytechip, LLC d/b/a Qbit." A true and correct copy of the original complaint and exhibits is attached as Exhibit O. Bytechip established a bank account as "Bytechip dba QbitPay" as set forth in the pleadings in the Bytechip Forfeiture Action. A true and correct copy of the complaint in that action is attached as Exhibit G and a true and correct copy of Bytechip's answer is attached hereto as Exhibit P.

105. Both Qbit and Bytechip are owned and operated by the same person, Yujun Wu. Yujun Wu is also listed as the CEO and the only member or manager in Bytechip's 2024 California Statement of Information (Exhibit F). This filing lists the address 620 Willowgate St., Apartment 2,

Mountain View, CA 94043 as both Bytechip's and Yujun Wu's address. Yujun Wu electronically signed the document on July 24, 2024.

106. Bytechip "dba QbitPay" listed Yujun Wu as the beneficial owner of a bank account opened in its name. Qbit and Bytechip have also had offices registered at the same California address. According to the Global LEI Index, Bytechip (Delaware file number 7363157) has a headquarters at 2381 Zanker Rd., Ste 110, Unit D, 95131, San Jose, CA. A copy of the relevant webpage, obtained from https://search.gleif.org/#/record/254900VKX1GAIRTC3F69, is attached hereto as Exhibit Q. On their contact page, Qbit lists one of their "Company Address[es]" as "Zanker Rd, Ste 110, San Jose, CA 95131."

107. In addition, there is evidence of Qbit and Bytechip's common digital infrastructure, suggesting closely tied ownership. For example, the computer infrastructure at IP address 13.114.27.194 has domain name resolutions to bytechip.co and qbitnetwork.com.

E. Bytechip/Qbit Cryptocurrency Laundering

1. <u>USA v. All Funds Deposited</u>

108. While doing business under its Bytechip name, Qbit settled the Bytechip Forfeiture Action with the United States after the US Attorney's Office seized Bytechip/Qbit controlled funds for suspected involvement in fraudulent activity and pig butchering. A true and correct copy of the stipulated settlement agreement entered in the case is attached as Exhibit R.

109. The U.S. Department of Justice initiated the Bytechip Forfeiture Action on January 22, 2024, to seize around $2.98 million held in an account owned by Bytechip and linked to fraudulent cryptocurrency transactions. The lawsuit, filed in the Western District of Tennessee, revealed that these funds were held in accounts at Evolve Bank and Trust ("EB&T"). EB&T offers banking as a service (BaaS) to different platforms, including Solid Financial Technologies ("Solidifi"). Solidifi in turn offered virtual accounts (vAccounts) to its customers, including Bytechip.

110. Evidence collected in preparation for the lawsuit strongly implicates Bytechip, Yujun Wu and his company doing business as Qbit in wire fraud and money laundering across the U.S. and Canada. In his Complaint for forfeiture, U.S. Attorney Ritz wrote of Bytechip:

> Based on my training and experience, I know . . . Bytechip['s] Solidfi vAccount **1162 **[is] used to provide money laundering infrastructure to a large wire fraud scheme perpetrated against numerous individuals.** Bytechip LLC, Gatcha Pictures, and Paralel Design are entities interconnected through IP addresses, outgoing debit transfers, and intrabank transfers of funds, **each performing an important function in a large fraud conspiracy ring.** None of these entities bears any indicia of legitimacy in its operations. . . **. I have demonstrated that wire fraud proceeds from pig butchering victims are frozen in . . . Bytechip Solidfi vAccount **1162**, and that these accounts are used to launder the proceeds of wire fraud.

111. On August 1, 2024, the United States of America and Bytechip filed a stipulated settlement agreement. The Court issued a Consent Order on August 22, 2024, accepting the terms of the stipulated settlement. Under the terms, Bytechip forfeited $542,728.30 previously held in its Solidfi vAccount. It also waived all ownership and relinquished all rights to an additional $672,493.69 held in a different Solidfi vAccount in the name of another defendant, for a total forfeiture of $1,215,221.99 (*See* Exhibit R.)

F. Defendant Qbit Financial Service's Role in The Present Scheme

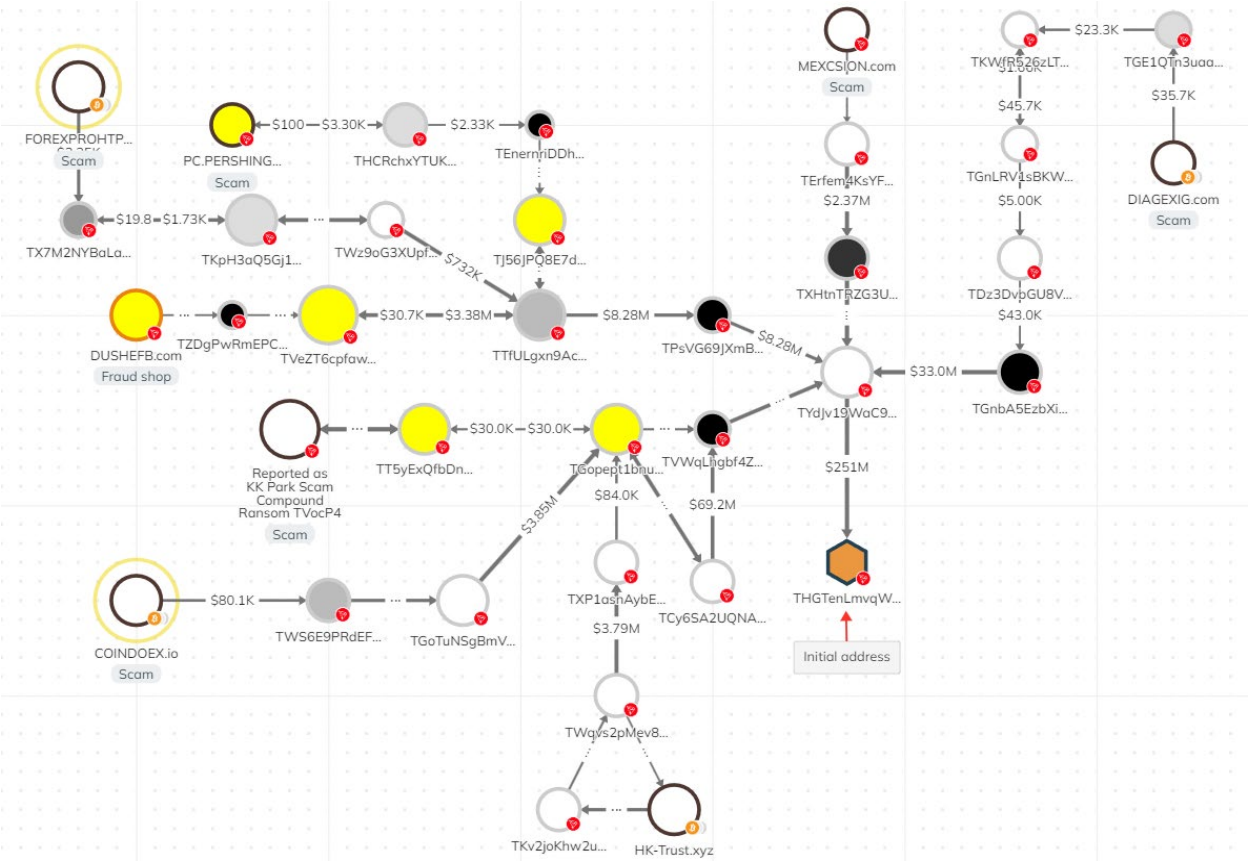
1. <u>Block Chain Analysis of Qbit's Wallets</u>

112. Qbit claims ownership of the THGTen Destination Wallet. From March 5 to June 6, 2024, $251 million in USDT flowed into Qbit's THGTen Destination Wallet. Nearly all incoming USDT deposits came from one wallet address: address TYdJv19WaC992rhseXA4j27R5FM2dKVDqk (the "Cregis Master Wallet"). In a November 7, 2024, letter, Qbit counsel claimed Qbit also owns the Cregis Master Wallet, referring to it as the "Master Cregis Account". (Exhibit D). The blockchain addresses attributed to both the THGTen Destination Wallet and Cregis Master Wallet exhibit patterns typical of scam addresses, including because of their multiple interactions with addresses reported in connection with various scam and fraud operations, as discussed infra.

113. Mr. Mashkevich's experts have traced cryptocurrency worth 7-figures in U.S. Dollar value to Qbit's THGTen Destination Wallet. Based on blockchain analysis of the THGTen Destination Wallet and related wallets, including those in the Laundering Network, it is highly likely that the wallet is used for illegitimate purposes, such as the provision of money laundering and other banking

services for scams. The Destination Wallets (including THGTen) serve a vital function as an off-ramp to turn the assets stolen from the Class into usable crypto- or fiat currency.

114. The graph below reflects a sample of Qbit's THGTen Destination Wallet's connections to seven different known or reported scams in close proximity (within seven hops) to the THGTen Destination Wallet. In total, there are 28 reported scam address interactions within seven hops of the THGTen Destination Wallet. The THGTen Destination Wallet is also within 3 hops of two entities sanctioned by the US Treasury Department's Office of Foreign Assets Control (OFAC). Overall, the THGTen Destination Wallet has exposure to 53 different reported scam addresses and 10 different reported fraud shops. For a full list of these addresses, see Table 1 and Table 2 in Appendix C.



115. Qbit's Cregis Master Wallet has received over 600 million USDT from a cluster of approximately 350 wallet addresses. Every wallet address that sent more than 1 million USDT to the Cregis Master Wallet received TRX for gas (transaction) fees from the same address: TGn4LVcWSPtnFev44viMNnwDfxnLa9zBQW ("TGN4LV"). Chainalysis Reactor tagged TGn4LV

as a scam wallet. It has similarly been tagged by two Open-Source Intelligence (OSINT) Comments for receiving funds from scams.

VIII. CLASS ACTION ALLEGATIONS

116. Plaintiff files this as a class action on behalf of himself and the following class:[21]

> all persons and entities who, at the suggestion of the Scammers or individuals acting under the Scammers' instruction or control, transferred cryptocurrency into one or more of the cryptocurrency wallets identified in Appendix A and other scam wallet addresses controlled by the Scammers as may be identified during discovery.

117. Excluded from the Class are the Court and its personnel and the Defendants and their officers, directors, employees, affiliates, legal representatives, predecessors, successors and assigns, and any entity in which any of them has a controlling interest.

118. The members of the Class are so numerous that joinder is impracticable.

119. Common questions of law and fact are apt to drive resolution of the case, exist as to all members of the Class, and predominate over any questions affecting solely individual members of the Class including, but not limited to, the following:

a. Whether the Defendants or their co-conspirators unlawfully obtained the Plaintiff's and Class Members' cryptocurrency;

b. Whether Defendants or their co-conspirators had a legal right to acquire Plaintiff's and Class Members' cryptocurrency;

c. Whether Defendants or their co-conspirators were unjustly enriched as a result of the transfer of the Plaintiff's and Class Members' cryptocurrency;

d. Whether Defendant or their co-conspirators s received from Plaintiff and the Class Members money and property intended to be used for the exclusive benefit of Plaintiff and the Class Members;

e. Whether Defendants or their co-conspirators withheld and converted to themselves the assets and property of Plaintiff and Class Members in a manner inconsistent with their property rights in those assets;

---

[21] Plaintiffs reserve the right to modify the Class and Subclass Definition at the class certification stage or as otherwise instructed by the Court.

f. Whether Plaintiff and Class Members have been deprived of the use of their assets and damaged as a result;

g. Whether Defendants knew or should have known they received money wrongfully obtained from Plaintiff and Class Members through unlawful conduct including but not limited to theft, fraud, or conversion;

h. Whether Defendants unfairly benefited by keeping the Plaintiff's and Class Members' funds at issue;

i. Whether Defendants' retention of the Plaintiff's and Class Members' assets is inequitable;

j. Whether Defendants' receipt and retention of the Plaintiff's and Class Members' funds in question caused Plaintiff and the Class Members financial harm; and

k. Whether Defendants acted with oppression, fraud, and malice, and with actual and constructive knowledge that the Plaintiff's and Class Members' assets were wrongfully converted by Defendants or their co-conspirators for their own personal use and without the knowledge of or approval by Plaintiff or the Class Members.

120. Plaintiff's claims are typical of the claims of other Class Members, as all members of the Class were similarly affected by Defendants' and their co-conspirators' wrongful conduct in violation of law, as complained of herein.

121. Plaintiff will fairly and adequately protect the interests of the Class Members and has retained counsel that is competent and experienced in class action litigation. Plaintiff has no interests that conflicts with, or is otherwise antagonistic to, the interests of other Class Members.

122. A class action is superior to all other available methods for the fair and efficient adjudication of this controversy since joinder of all members is impracticable. Further, as the damages that individual Class Members have suffered may be relatively small, the expense and burden of individual litigation make it impossible for Class members to individually redress the wrongs done to them, especially given the complex and convoluted details of the scheme at issue. There will be no undue difficulty in management of this action as a class action.

IX. TOLLING

123. Any applicable statute of limitations has been tolled by Defendants' knowing and active concealment of the conduct and misrepresentations and omissions alleged herein. Through no fault or lack of diligence, Plaintiff and the Class Members were deceived and could not reasonably discover Defendants' and their co-conspirators deception and unlawful conduct.

124. Plaintiff and the Class Members did not discover and did not know of any facts that would have caused a reasonable person to suspect that Defendants or their co-conspirators were acting unlawfully and in the manner alleged herein. As alleged herein, the representations made by the Scammers were material to Plaintiff and the Class Members at all relevant times. Within the time period of any applicable statutes of limitations, Plaintiff and the Class Members could not have discovered through the exercise of reasonable diligence the alleged wrongful conduct.

125. Defendants knowingly, actively, affirmatively and/or negligently concealed the facts alleged herein. Plaintiff and the Class Members reasonably relied on the Scammers concealment.

126. Further, Defendants' unlawful conduct was done surreptitiously. As a result, despite Plaintiff's and the Class Members' exercise of due diligence, they could not, and did not, discover the unlawful conduct described herein.

127. For these reasons, all applicable statutes of limitation have been tolled based on the discovery rule and Defendants' concealment, and Defendants should be estopped from relying on any statutes of limitations in defense of this action.

X. CAUSES OF ACTION

FIRST CAUSE OF ACTION

(For Civil Theft Under California Penal Code § 496)

128. Plaintiff re-alleges each paragraph of this Complaint as if fully set forth herein.

129. Plaintiff and Class Members owned or and had a right to possess certain digital assets that were fraudulently obtained and subsequently deposited into accounts controlled by Defendants.

130. Defendants received, concealed, or withheld or aided in concealing or withholding the stolen digital assets, despite knowing that the digital assets were stolen or obtained in a manner constituting theft or extortion.

131. As a direct and proximate result of Defendants' conduct, Plaintiff and the Class have suffered economic harm.

132. Pursuant to California Penal Code § 496(c), Plaintiff is entitled to: treble damages, attorney's fees and costs, and any other relief the Court deems just and proper.

SECOND CAUSE OF ACTION

(For Unjust Enrichment)

133. Plaintiff re-alleges each paragraph of this Complaint as if fully set forth herein.

134. As described more fully above, Defendants either directly or indirectly received from Plaintiff and the Class Members money and property intended to be used for the exclusive benefit of Plaintiff and the Class Members.

135. Defendants knew or should have known they received money wrongly obtained from Plaintiff and the Class Members through unlawful conduct including but not limited to theft, fraud, or conversion.

136. Defendants unfairly benefited at Plaintiff's and the Class Members' expense by keeping the stolen funds.

137. Defendants' retention of Plaintiff's and the Class Members' assets is inequitable.

138. Defendants' wrongful receipt and retention of these funds caused Plaintiff and the Class Members financial harm.

139. As a result of the foregoing, Plaintiff and the Class Members have been damaged in an amount to be established at trial and request restitution of the stolen funds, plus interest, in addition to appropriate equitable relief, including but not limited to entry of a preliminary and permanent injunction that seizes and returns to Plaintiff and the Class Members the cryptocurrency assets contained in the cryptocurrency contained in the THGTen Destination Wallet or other wallets held at OKX and controlled by Defendants.

THIRD CAUSE OF ACTION

(For Replevin)

140. Plaintiff and Class Members are the rightful owners of certain digital assets, specifically cryptocurrency, that is currently wrongfully held by Defendant Qbit.

141. Defendants have unlawfully taken and/or continue to wrongfully detain these assets, despite Plaintiff's and the Class's lawful right to possession.

142. Defendant's wrongful possession has deprived Plaintiff of the use and enjoyment of the assets, causing significant financial harm.

143. Plaintiff seeks the immediate return of the digital assets, or, if return is not possible, monetary damages equivalent to the value of the assets wrongfully retained.

FOURTH CAUSE OF ACTION

(For Conversion)

144. Plaintiff re-alleges each paragraph of this Complaint as if fully set forth herein.

145. Plaintiff and the other members of the Class transferred assets owned by them to Defendants.

146. Defendants wrongfully withheld and converted to themselves the assets and property of Plaintiff and the other members of the Class in a manner inconsistent with their property rights in those assets.

147. As a result of the foregoing, Plaintiff and the other members of the Class have been deprived of the use of the above assets and damaged in an amount to be established at trial.

148. The above-described conduct of Defendants was made with oppression, fraud, and malice, and with actual and constructive knowledge that the assets were wrongfully converted by Defendants for their own personal use and without the knowledge of or approval by Plaintiff or the other members of the Class.

149. Plaintiff, on behalf of himself and the Class Members, accordingly requests imposition of compensatory damages, in addition to exemplary and punitive damages, against Defendants, as well as appropriate equitable relief, including but not limited to entry of a preliminary and permanent injunction that seizes and returns to Plaintiff and the other members of the Class the cryptocurrency assets contained in the THGTen Destination Wallet or other wallets held at OKX and controlled by Defendants.

FIFTH CAUSE OF ACTION

(For Money Had and Received)

150. Plaintiff re-alleges each paragraph of this Complaint as if fully set forth herein.

151. As described more fully above, Defendants received from Plaintiff and the Class Members money and property intended to be used for the exclusive benefit of Plaintiff and the Class Members.

152. Defendants did not, in fact, use the money and property received from Plaintiff and the Class Members for their benefit, but instead used that money for themselves.

153. As a result of the foregoing, Plaintiff and the Class Members have been damaged in an amount to be established at trial, and request compensatory damages of this amount in addition to appropriate equitable relief including, but not limited to, entry of a preliminary and permanent injunction that seizes and returns to Plaintiff and the Class Members their cryptocurrency assets contained in the THGTen Destination Wallet or other wallets held at OKX and controlled by Defendants.

SIXTH CAUSE OF ACTION

(For Aiding and Abetting)

154. Plaintiff re-alleges each paragraph of this Complaint as if fully set forth herein.

155. As described more fully above, one or more Defendants unlawfully obtained Plaintiff and other Class Members' money and property.

156. The Defendants knew about the wrongful conduct and intentionally provided substantial assistance or encouragement to facilitate Defendants' wrongful receipt and retention of Plaintiff and other Class Members' funds.

157. Defendants facilitated the theft and concealment by receiving, transferring, laundering, or helping move stolen funds.

158. Defendants' assistance played a critical role in enabling and furthering the pig butchering scheme detailed herein.

159. As a result of the foregoing, Plaintiff and the Class Members have been damaged in an amount to be established at trial and request compensatory damages of this amount in addition to

appropriate equitable relief, including, but not limited to, entry of a preliminary and permanent injunction that seizes and returns to Plaintiff and the Class Members their cryptocurrency assets contained in the THGTen Destination Wallet or other wallets held at OKX and controlled by Defendants.

SEVENTH CAUSE OF ACTION

(For Civil Conspiracy)

160. Plaintiff re-alleges each paragraph of this Complaint as if fully set forth herein.

161. Defendants agreed with unknown parties to engage in unlawful acts, including theft, conversion, fraud, and money laundering.

162. Defendants intentionally took steps to further the conspiracy, including by: wrongfully taking possession of Plaintiff's and other Class Members' funds; accepting wrongfully obtained funds with knowledge of their illicit source; transferring, concealing, and laundering funds to prevent Plaintiff's and other Class Members' recovery of the funds; and participating in or facilitating fraudulent financial transactions to hide the source of the wrongfully obtained funds and to prevent Plaintiff's and the Class Members' recovery of them.

163. Defendants knowingly participated in the scheme and acted to benefit themselves or other co-conspirators.

164. As a result of the foregoing, Plaintiff and the Class Members have been damaged in an amount to be established at trial and request compensatory damages of this amount in addition to appropriate equitable relief including, but not limited to, entry of a preliminary and permanent injunction that seizes and returns to Plaintiff and the Class their cryptocurrency assets contained in the THGTen Destination Wallet or other wallets held at OKX and controlled by Defendants.

XI. PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for an award against Defendants as follows:

1. Certify the proposed Class, designating Plaintiff as the named representative of the Class, and designating the undersigned as Class Counsel;

2. For compensatory damages in an amount to be determined at trial, in excess of $28 million,;

3. For an award to Plaintiff and the Class of equitable restitution, including the return to Plaintiff and the Class of all cryptocurrency taken from them in connection with the scheme alleged herein;

4. Punitive damages in an amount to be determined at trial, not less than $50 million;

5. Temporary, preliminary, and permanent injunctive relief, including enjoining the transfer or dissipation of property and funds held in any wallet own or controlled by any Defendant including the THGTen Destination Wallet and the Master Cregis Wallet;

6. Impose a constructive trust over, and order the return to Plaintiff and the Class, all stolen assets and proceeds that are held by any Defendant;

7. Statutory treble damages under California Penal Code § 496;

8. For attorney's fees and costs of suit;

9. Pre- and post-judgment interest; and

10. For such other and further relief as this Court deems just and proper.

XII. DEMAND FOR JURY TRIAL

Pursuant to F.R.C.P. Rule 38, Plaintiff, on behalf of himself and the Class, demands a trial by jury of any and all issues in this action so triable of right.

DATED: March 14, 2025

KURICHETY LAW PC

By: /s/ Vijay J. Rajagopal
Vijay J. Rajagopal

ESBROOK P.C.
Michael Kozlowski (to be admitted *pro hac vice*)

Attorneys for Plaintiff
MICHAEL MASHKEVICH

Appendix A

Deposit Wallets

1. 0x6177c7906e9534b88dc78BA09b6627064543D364
2. 0xC0B40da64b9e2552FC7F9a61FF80764625536950
3. 0xc75326a8fA226857474624ee00CbBe309439785d
4. 0x368180d4E9170f86952182328cd86ccd343A83FB
5. 0x0683FF8E842081bA091E59ae73BBcc3FFfe74e76
6. 0x8dD60CCFCA1d0Bd1DC58F1ce44987C3459857bb3
7. 0xa456e853C6b428c177325a0D326295Fc4a6fC1B4
8. 0x31f7c7068BcaaC42bF7eC48E27c1bd8b2307A190
9. 0xF46D4D4f60510c1eA1B4c29AF2781bfb66374298
10. 0x5Edc5c6F087165098601A07f76Aa4d6455f43924
11. 0xB03E5A58b4C7608468300fa6be0BaA28422A7cAe
12. 0x788D706fEd25752A304c3F8439961B1BFF461b44
13. 0x3a76d3eA63076d820E801bbe7a2C4Eb50105E40a
14. 0x8606DfF9FCeFF596e9E2a0508d2a8fCBa54C96Fa
15. 0x0C07a5323611b2Af48149cA133b9f93Dcbdb0610
16. 0x166e50dC04f1A95bD9d60639Bc450a5d2751ba84
17. 0xA51264b36311Fc74901F5f2a3c9C977faE7e4f66
18. 0x4C0326787c6319d6C758a94aEc00E27Df82ca47D
19. 0x75F93605A3f91f694cE6C99065814388d69B2D0a
20. 0x7a5325fBAF365F00bc3f5918cdf2EDB15F139895
21. 0xE038982728E476A5a98543BB27A0b8407Cbd2260
22. 0x63e9d03C1b8c2d541632B3032b90b137c349d08A
23. 0xa71D6B032217C09fB37ee48dc2Cb4aE77f1c8474
24. 0x5646f30A794032Ff3b9D76A8fcfeA8d708aAaE0d
25. 0xc17897a1702947ECA8a5Da3D9A1Ac3f39acfa3b5
26. 0x35ED5743f3af5FcED1315d05c64a850961F7e440
27. 0xe1bc2D1F20f633eDa9d31a871768D492B3D5F5ee
28. 0x914068a2083B7657102382500508bA16db4692d9
29. 0x494A4164A33216952be34d2a6DD6f5F1be899C53
30. 0x4b3BD2Ba74200e586B18181eC9930ed40ab2C27E
31. 0x56f79bdEc7D332ecEE4899B4E286a86822a7B581
32. 0xA6B9487D5e2602080b4B3bD751eA39987c25E657
33. 0xeb116C42697CaE28621d6Cdc7283f018645a078a
34. 0xf8E4B383270FB912F5CAdfA129afFa6b19261A01
35. 0x6Dee34D8cA306E97f7C3E7E6405516E88E6B83F8
36. 0x608D221813f28416E0D954a832102C3c3De36992
37. 0xB680B6c4875a57a30c367fBab6f4D1F0991e58Fe
38. 0xE6cdFbDD5a2c824A65Cf5d60d463a1C2adcb7e72
39. 0xc3c471d71FF91BEE8bFda547C9b3df5967c11415
40. 0x23152378866694c5AE067d43f847D5aA656b3573

41. 0xe77D16C7b1DdE5702DF21CCc2240cC2EF55d8bA6
42. 0x314EA4706708A32b71970C3e767229a8e85106B1
43. 0xe42AE0C6DDdA371Ea62059505c446F74Cb252Ef2
44. 0x7d5CBD7175F3ede95eB21F00dCB4883dd87F72Da
45. 0xAE916F6FB834eF747233e5Ca38c470f0B070dd02
46. 0x55622d6028215942a047dBC2BAc7C7c136D45868
47. 0xB2a15992E74e712065F352B62de845017718B260
48. 0x47AF4c88b9D8376a9523e2d36e38a37C87fB42c9
49. 0x26Bf00Df1507c3B427f31b765C3Ffa53Ae4dfd87
50. 0x6C188BC54491a9Caed91b087151902FAC40646B7
51. 0x97e062Ac68725F1f7D14F06FE4d443164bA4cd37
52. 0xE157F32D364927b99b98D74902cCD06D1089D771
53. 0x689188D09AaA1B0A1Ad74008D60a62917DDF040e
54. 0xc88ceeF1ff20aa9938144c18b04d439640de4a16
55. 0x4cCc9c25E32d72A48bc6fDa08846404EEB504e3f
56. 0x3Ad4a8Ab2C6d5bC936EC817c5A33e8C74802e743
57. 0xfBd4Fb2E25E36bE7fc27452626Fe1479F909E886
58. 0xBBD29055b4D9863fC0f2B6523E2e2BEF2F5B59fE
59. 0x2508063f8784a713Eed9B3Df9eE6e62e3A885AFe
60. 0xaB951C29e9841D08bcc44Ab45216056067591641
61. 0x9FC0848ADCee1a88b554dd0326F1D9AA1B65E780
62. 0x18225C97ed2D8770c580f9c0Fe501b93514F4A1D
63. 0xc48996D440Aff63DB7A646Cfbf20F2c0B2F7876e
64. 0x77ddc787b489d076b6041E7e4D42C6cfc32b6340
65. 0xb175e09057dD62D522732667BE3Bd27C7e4B4eB4
66. 0xCE5DAE0cA663Ad15Bd5A086e736a60a88417313a
67. 0xC14367c9978d969BF45b732f4d4DBcb61DaD0824
68. 0x2fc4dEeE44BAC31228a698FC84A4B08bEefeCB26
69. 0xA47973BB1A9BcaC12efFd739216b4F6a9F60CFC9
70. 0x7c96ADc3f58576fD8F79fE526EB77F7279B47Dc6
71. 0x1C6857d01E4C40D8F22B73f6d8AD074f0d166574
72. 0x3B9C9a8363bF60193505F353854D2f3D52F9b2e0
73. 0x03C3968D7adB9926542e61066d02D326c32114e4
74. 0x154c0c0e799E6B7eb5e7452B3A3Cf06e0E07d628
75. 0x8bD597497A9095eec1FAC2A30d3bDee770F63F3B
76. 0x04694d093644ce00d11d41b609d7C45a39849b48
77. 0x6504D4888d0d47C92695A70917Bb7363fC348846
78. 0xAc1c75687DD3742BcC80bA7f74f3791a270D59a3
79. 0x716A9B0661979066eF860Be452F2271ae984bd12
80. 0x0597C577DC7FD0F41111de2B75BAa0E82068D93E
81. 0xc13E7e85Fdc7B97Ef7633767c306f5877e2a76C7
82. 0x4c5f0119a2e97C811728ff26F937eC8f57678cCa
83. 0x3A4E7B9AEe300E7B4896EA68013599Ed0F0Fad6C
84. 0x222cF7A0498AcEaFaCc23467D802B59E2A78923a
85. 0xFC73E5a31D74b8b40A437f6eb548A621D358DaF9
86. 0x2f90Eee546B00F030f8D422e8d5217b89035913d
87. 0xCf36372A55A522f9c0235CDc3A1C28A157095d03
88. 0x0F8e2F3dde416acAc21B13796913Ba7a86C6Cb20

89. 0x5A7eBa3EDEC3eACFe3AfBEA5D5c712a6Ec4c1f08
90. 0xA3970d3b1390492cf6c1C39Af0F07d7469870E47
91. 0x5545A5DD2AD92500e9413801203c381B964E8cfD
92. 0xbf05480F77De26926EE0D2edDe37F383F9f33D59
93. 0xD331Bbf9F95e4dF036c007c76bcDe27471D17103
94. 0x7556e23cE4C796e29F18E25753323d614490c936
95. 0x3B9ECe84F4a7550fb7d0F5e14260673461f6DC7c
96. 0xb7108cf35DE32f012Fa92Ce5602b154185b2D408
97. 0x508f7fF93e15438d41C9Ac596A8d848a29520A91
98. 0x3bf46C2F5A784B32Afd3a54c87863F01ed711541
99. 0xBCAec63946CC1B0eD9646E6c1b1eF645BaA3e360
100. 0x47462B6BD435634b61F9208A8B2f09B789953244
101. 0x435509F2B1a70578ff52F990cA0E000d4AE2B8D9
102. 0x00d7566C469B5936B720b589afbAD47f646b954F
103. 0x37489982B4E2DfF94BF7D04D8031541ce76e40E2
104. 0x60DBDf08B15F4722259097635901A042eb6c3fa0
105. 0xa7e874E0A24f45A9D5EC67Fd63290D341D8b404A
106. 0x3C6Df4ea6B9247215bb462DC9219e6082467460b
107. 0x0dB70a34000bAE8fd6A98E99795EcD4B2f658027
108. 0xD8c4F003DB1a6c383566779cdbFe16a6018906dB
109. 0x9E3a3E6D78F940da2c11F00707DE485C465D5646
110. 0xE04f5B6F583f5fE25268480E277599C83206D7Ed
111. 0xF8c1E5116eDE63BDB09E8a820A2d26d106beb8d3
112. 0xBabdA434461D06dC11a527994E81CADF9D3C6035
113. 0x1bC92c85EC52758549843A26Ec3d07D8384Ff53f
114. 0x80bb9FBf37851454E1837E5fCAb63eECc3086a00
115. 0x4f6901869ABB1d980CBaf388e8B1dDeE25852213
116. 0x0E0bdFc5A9bD733c2F20906428795D1553C1bd24
117. 0xA5574C3fBf47060Fcd4e92C87983f3BB55BE7692
118. 0xa5E9C89f672E8A4cbF2f346FEcD1F277E6C78006
119. 0x42a77d515AE8271c6b8cE2B5016f58990999A629
120. 0xafb4b09274B8c76eD20773859e01859CfeCb49B3
121. 0x56F53Ad3B7C4c190000D9584f4687089e9DA0822
122. 0xF6c33eD5A930441B84AE52Ed667c7D77dDEC953f
123. 0x5547e1587E8a17f6264C97Bf4dC20630aaf3B39f
124. 0x67C05A92741A5D10c6AAcFE02682E69D22c087B0
125. 0xcd39992DBcc6F2aAdfC53A370644fB4F6E74E271
126. 0xf834583E2844AC2262aB52d4B943cb24A4328324
127. 0x76DEF9C3194CbE6c857BE24980729913aFd50272
128. 0xF915dB509Ca5f93A213a9e121e69e6D36037eF2f
129. 0xa600A68Ca3970C6fAAF4288E728638ca6ce397c4
130. 0x9D67d9Aba4e330c7FA578643F99d95f653924dd7
131. 0xba025601D82D7c048C18a649098b25d6CdD7E978
132. 0xbCB8A3cdC099B8bc692D1ba393ee6Dfa57e3b60a
133. 0x90ef6046c1e43ce33DB6930b6ae46d94D4D366C5
134. 0xED10896919D5E57dE28803be4c0804AE5D12F132
135. 0x7b00c4eA329eF0892443D0ff124aD247955eA49A
136. 0xd4547A063130Bda8580Baaf671c5C525912B32B0

137. 0x9c06EcdF4D089db538EF95729eC5A29d7B3684E2
138. 0xD0291B33D17bC267c2cc3E18320B71f6623e7a6B
139. 0xD409Dc76eA77a45372fE9640B09c5381C057C8FF
140. 0xB84028b16F874F0D50FE7EAfcB77393c0bB918C9
141. 0xa926E550C88Db2f84e35390c03c604dF2645c862
142. 0x18Ba14C97a61bBbaB890eABcE3F4Ae3Ac16f2299
143. 0x37206199b8e90bC7037a4395Ab26A95c066737cC
144. 0x6524F4A1e721d70F0a05598626FF5A8D9219e55C
145. 0x73D873CbB8D564622759ED7e50DFf8046Ba36B0d
146. 0x31C13583a64c51ed6650A1b3Fb3ad62C7A9f09ec
147. 0x3eaCdfd2d9C6a6408BE4Bab0198a234B4AA43086
148. 0x04d20cD20739bEf0F80ae9df46270BF22FD215Ab
149. 0xbDb79488c86602779efE3D6aaB1bd6b7EfC55E12
150. 0xbe79342e98Aa86Bf94e5F303A4bB904B764542dc
151. 0x8EF1fa30ff5c2eA66d7D80f93FF7dD00692EEc67
152. 0x24e94718A6BDDc37004Fe250521F6721FfE359Ec
153. 0xA02F6FD865C70e95287634249288F1ED995d20f7
154. 0xfAcdF092F8f3139A519f5BE5EAd6d0a01D0D69b1
155. 0x18F6398D89dbE387E511a01eAC9FD9405bE8759B
156. 0xD77801bcd13f03b3327E943Ba38D14C44D97d13F
157. 0xFbA63A440D1ca445f226cc988d4a125a29d07940
158. 0xA00FA50a3c59c5a6F8BaF414560766150418AAE4
159. 0x98B33317560534cfFA7803b5F260834081C71aB2
160. 0xCae47fdD296d54aAaC6694256c892B2F913CcdfE
161. 0x6De0dd7FF1d946166092fE2E5C612aD2A8Ac4601
162. 0x1F972cB388CB57266E74116C31CEF3B9e7880960
163. 0x8bDE39e942435d44AcDe50baCd310Cab903C9eE2
164. 0xD001a56e92Ca23efd129a649ecB7B524260B0E2f
165. 0x8B992782f8A2E4B11c14Fda55630C9Ba9B9aF8e5
166. 0x527cc1BE2652D37c0B8703d7e5B62914C39E2577
167. 0x937fde13236A06EbFDcd73e0ff943475375cCee1
168. 0x4c2de28F9aDabfA7377199A2D3CE6F747615f441
169. 0x961509dF10bE2b6c661be73C9363c6B0DE3FEd8f
170. 0xC832b8593b96bb25B59AD482b7A48f735b872963
171. 0x96B5EbE0385F7e4583B0b66590531836C0309DC5
172. 0xb1A8c74Bb945107Bb114ED20eE03D1A3695A18e5
173. 0xC21e7E2c67Ba38062D6B831D33c9fA54aabe34BE
174. 0xc7299032c1A14a5802aF2c33f14660D88241505C
175. 0xddEb8338845c0e333684187874E664A5FC262b66
176. 0x670bb8492eFb21e56D673C7a62d23205A8a54B92
177. 0x8ab4f99C8fA3802F85ea46D5Ab30a1D55265e93e
178. 0xe9dcE0C86dd50AB6282D4Ce325181801858a6dAC
179. 0x8a018D8049Ef33Aa7E243392695b7B0dC1ecE265
180. 0x98f793A2c5AF7fC2Deb88c67591C17cF0c4D4E2d
181. 0xc2A0a868295436568B7CD4069Ac343b868eD2Cd2
182. 0xdf9e43880be62Ce20F9D0EB53F7C7E45F8B5D866
183. 0x0f6E73841D61ade33a09912651848E2826431e1D
184. 0x5258cB0D4d79F22F617d6d990C3dD7E4753c46f2

185. 0xED2Ae70A34DdFe7e11DB3852eeea2822AC783729
186. 0xc281ca7C69E7c60c400831a197Eb4fDaEB18e583
187. 0xBaA927a6D60D26E9D19c722d5faA4F2Abd7d6929
188. 0xB139898b89A34c0da181aABD678a93C2DA68Ad5a
189. 0xbD3D2A7a8e3A4b53cdE9Ede19FC3FecfED8A37d1
190. 0x1F2F23fB853f7E1eB0c831060Bf82299bf9a0103
191. 0x9504c6111672170CA96C597D5D1f41ad5dC05343
192. 0x0EBC6fE0593E68388a1dF7ac4D6e0814Ca9AeBc9
193. 0x08DB393CDA7C853B8d3A21eD5cd4FF5D843ff33f
194. 0x96f62dc3B3D45Eea138e66d38F95c224eddFB8D3
195. 0xF3Dd242F331a62b2dd3eC23F817568F40DdAeA33
196. 0x88Ec5F5A9becdb5f7A5c42E88d49Dc2975e194B1
197. 0x351B64b04D1f55B249fFbf83D6458148d650808d
198. 0x17f12314993CCBF13bb569F18969C751ae9c695D
199. 0xd8a644c6f319BE9dA79A0dD09d14E1af9E15090d
200. 0xbdD68C08c7513A69a3329865cB1F9D2E90A33Bde
201. 0xaf177daD83F36Acd106d666F829d57C0d52e144F
202. 0x5618513c997e5Ae3A7295FF0878aFEd0Dda84534
203. 0xfD5c4BeaA54296999e01c613db09Bbc11273e237
204. 0x413cF16c6da30c75db41616ace10e982D25D3FE2
205. 0xee65DEED460F047F667FbCC4196E0551f7eCCf3C
206. 0x2d69348985D1d2EBb304B6F3ff8635B9cae2320d
207. 0x4b3CB270A6b6ef603998dc4A6b4b66711A2E62C0
208. 0x9D6A2d3F052cc9372318EC93690D60D4a5118A78
209. 0x86d912e00229220f904397932855806d6403Af6C
210. 0xF55ad3f4Cbca16B0D8DbCCd51429C54C6A2B7fbE
211. 0x30821da4b6cae094b3026eDBb390d9461289A4df
212. 0x56AcE8884507982C818DcCBa9D3E2Cc95A2061c0
213. 0x6e8d5211c810055bdf11539DAb25089BffFFB092
214. 0x59c82203228506Ec19a8036Ee38373F8771cDB38
215. 0xC45a1c6E33fd5CC2e0C039A16aDa9bC07A58668C
216. 0xcb27ac7761F0878cE65Fdd4E24d6f831acC0C0f1
217. 0x5D6B701E141bB50753d7A6D4ca09337DE31c7619
218. 0xa8f48dB1E1fc2E933D9E1beEFA492ab5A482C4Ef
219. 0xa16F318Fa0C63C304DE8FF5Ba1D7ef8B1596a6bd
220. 0xFE923588d09F129106Dfa29eEfd025e328DBFf4f
221. 0x7f44b3a68B21AE5eC56723a6b85303dF8D792B5C
222. 0xaC7f90D3Ee4D16a2421f3d44C80973dC612f48c3
223. 0x9E8154Dea58b56efC4944325Af6c7D2122Bc1e0e
224. 0xCDf21C6390C84cb91C3153E0Fb5B88D8AaA576d6
225. 0x683403344c013b3129ddAfe425dC46f9BfFf3dC9
226. 0x30962D1d7eaAe6C4051F7B6242e7824E84148376
227. 0xb0E5461254479a50c6914c1A1B6840C352406452
228. 0x784dF3f96314571125ddbB75d1387FE1B9AFF1Ca
229. 0xF431ECc9a4D1c562B459029eE98eb98573965a16
230. 0x3343E36499Fe1c9f2A7B793D4d5A6C3287F2eF0C
231. 0xDb51e909e5866FaF7a44423A49d8BFd61Eff421C
232. 0x291a01db06f3f1DF03FB4b7E7e01430a4230Fbb5

233. 0xd3a6A07e974118c68D55A8fE307AdA8b9b7153Fb
234. 0x1F88c0252282a4b59de7896eAde9E28e9891B4f2
235. 0x672A0bAE90828677a0F93e012FdE1914375DbCaB
236. 0xB146736170B0C37965F704D022a80dA128AF8A97
237. 0x0B5f9B23dFa28397aE7C673d590571882E78A6Fb
238. 0x57c1d519EF2A29689Be9186AB08574634C1ccCB6

Appendix B

Destination Wallets

Frozen in Alabama Civil Action Number 50-CV-2024-900163.00

Binance

THm7R5wHvqx8gZkCX9KS9hjhvUv5TrXU4y

TTTkoMc9VuVKTGFQJPxF5pS2f1XV5u5QHJ

TLB95AHgDtns5cohFKicTsE2zpFqcbzMM7

TBeUKtZxjcR6HmeVXV4TFeFWN3nvDDAqTw

TXMA8WaXdWa5EYkBhAMuCwjHjSdHGvyV2y

TCzHEWKCgo17CVwbkPFmZorDi9kWkpMbnd

TKJ77SjyQGAX4u711tneGXpgZLTVwRZ8Uk

TFsZ9UvNYS4tLPWLUzKsGviHsPsWFuKsH8

TPJV9ayW6YqPK9yddvaMzKwm424ySeJriK

TNRzzzCZ5x1HPS6LSca2MCamDLoJNQLTdW

TDuJLcreNwBzDp3RHrpsoTbhnw9s3QmPb9

TBJh9brKQp8ZvTq6vi5BvU9epdwEP63ysj

TWUeDMvPrY88cpX2EmFxHdd2xtWfm9cPDK

TLvFAMp7qZ7iF8fqqewM7AMjJtzZwjSWve

TGqjuFc8jxfjZBpUuFGnRLAXqzbHzYB4Wm

TLN6ayhvQqzFK1KweyNDfMiqMfgrZ2rMg3

TUjGaqLmBnYythnN5hPNELyJPBBmEcjXdW

TTv4AqmaKwMt2SagrSyRyqE7XB6dpLUHyd

THEJ47jWuKmwssvvo7hrmw1wyjFbxDR54p

TP9uatVfbAcZe4qAqANZ6Hjc7JrzGGYhro

TJphKU7t3aW1WoJ3ur9YW4zxNwE9cc6e2H

OKX

TSLj5S3KAfvK8mDtDBisZvWDGUbKUDR16v

TCeLkTvsCb6Tz2ik7xng1YoT9BYdcVxHnr

TJGebBJfUAgs4NUManaRFGQRpoLEwYPj2o

TLXtzgg2Axd7ThhhZRq5LoBLgsUYnx8TpZ

THGTenLmvqWycGLGtgRvX4wURiHQeDvNps

TFwi8cW7CUZ3mVY92hYaQiEoAYr5z1E2Kh

TUxrJsf1ZcRgXpfX9L2VLUCEJ5DUs2mWC7

TKuKfiyMCV65AK4A5YGLP3sgDnzkMc6fdp

TA8C3BnEyVvyPGTTEhcsNZz9jNNm6j8tbi

Gate.io

TXV4pAhJSk9BxetRLh2BvTEnyC8xc7VZM8

KuCoin

TDGGk3yNwo9uEmL69zmdwJwUYaCozZMQuD

TUijurbvTKwCpYzEi3TnC62gRLGCxn7q6T

LBank

TUNN5XDrQg6fkfUEdWcYDHgvPwXyxS1k2C

TGUSM4zJ6XrJ5xaD9pnB5eLrKy2GqjG3pC

TVXe59tPrQmFVrP4no59t1Vp3aDSfs8m2t

Appendix C

Table 1. List of scam related activities connected to Qbit's THGTen Destination Wallet

№	Name of entity	Type of activity	Number of hops
1.1	MEXCSION.com	Scam	4
1.2	BTMAEX.co	Scam	4
1.3	KSRSRA.com	Scam	4
1.4	EIKFOXEX.com	Scam	5
1.5	KK Park Scam Compound Ransom	Scam	5
1.6	M.ENROLLBANK.com	Scam	5
1.7	SGXCOINS.com	Scam	5
1.8	AIYFPROEX.com	Scam	6
1.9	COINDOEX.io	Scam	6
1.10	HELIOJW.com	Scam	6
1.11	DIAGEXIG.com	Scam	6
1.12	ZENEXCU.com	Scam	6
1.13	TDSREXPTO.com	Scam	6
1.14	ABUSA.cc	Scam	6
1.15	HFM.HDTUKC.com	Scam	6
1.16	M.SOLUTIONSFX.cc	Scam	6
1.17	AIYFPRO.com	Scam	6

№	Name of entity	Type of activity	Number of hops
1.18	KFGIT.cc	Scam	6
1.19	MCDEX.buzz	Scam	6
1.20	DecredGPT.com	Scam	6
1.21	HK-Trust.xyz	Scam	7
1.22	FOREXPROHTP.com	Scam	7
1.23	gndjk.com	Scam	7
1.24	PC.PERSHINGMENTLTD.com	Scam	7
1.25	KEN-EXS.com	Scam	7
1.26	app.guojkol.com	Scam	7
1.27	decxauait.com	Scam	7
1.28	Space-Contract.com	Scam	7
1.29	Reported as fraud TTBnMQ	Scam	8
1.30	MTFE.ca	Scam	8
1.31	bkextra.com	Scam	8
1.32	DigitalTurbine-Web.com	Scam	8
1.33	MKXPROIN.com	Scam	8
1.34	TRUST-AMM.com	Scam	8
1.35	Bora.band	Scam	8

№	Name of entity	Type of activity	Number of hops
1.36	FXCORP.cc	Scam	8
1.37	NMDABD.com	Scam	9
1.38	fffhna.top	Scam	9
1.39	OrbitzShop	Scam	9
1.40	SCYMAXS.com	Scam	9
1.41	BCTRADE.store	Scam	9
1.42	OKTEXA.com	Scam	9
1.43	WeAreAllSatoshi.org	Scam	9
1.44	WEB.FOUNDRYUS.com	Scam	9
1.45	WISECOINAAVE.com	Scam	9
1.46	DigitalSilk-us.com	Scam	10
1.47	Octobits - Telegram Bot	Scam	10
1.48	ZOOEXE.com	Scam	10
1.49	2139.com	Scam	11
1.50	TNZJWNKJ.com	Scam	11
1.51	WNIUVND.com	Scam	11
1.52	YCOINTO.com	Scam	12
1.53	Daisyforex.org	Scam	14

Table 2. List of fraud related activities connected to Qbit's THGTen Destination Wallet

№	Name of entity	Type of activity	Number of hops
2.1	387585.com	Fraud shop	4
2.2	TINDER1.xyz	Fraud shop	4
2.3	WY.67DS.top	Fraud shop	4
2.4	DUSHEFB.com	Fraud shop	6
2.5	DANAIVIP.com	Fraud shop	6
2.6	YF77688.com	Fraud shop	6
2.7	Matches-Millions of bases - Matchesbabycc	Fraud shop	6
2.8	YSS16888.com	Fraud shop	7
2.9	NISUS818.com	Fraud shop	7
2.10	XJQVIP.com	Fraud shop	7

Appendix D

Wallets on the Ethereum Blockchain from Victims to Qbit's THGTen Destination Wallet

Initial wallets (Plaintiff):

0xD4698477E65C7be219094aC71F65F40582EF5dbe

0xFBee5baBA85C839e3E6aBD11b7eF4D8001357f82

Pivot addresses:

0x30962D1d7eaAe6C4051F7B6242e7824E84148376

0xb0E5461254479a50c6914c1A1B6840C352406452

0x784dF3f96314571125ddbB75d1387FE1B9AFF1Ca

0xF431ECc9a4D1c562B459029eE98eb98573965a16

0x3343E36499Fe1c9f2A7B793D4d5A6C3287F2eF0C

0xDb51e909e5866FaF7a44423A49d8BFd61Eff421C

0x291a01db06f3f1DF03FB4b7E7e01430a4230Fbb5

0xd3a6A07e974118c68D55A8fE307AdA8b9b7153Fb

0x1F88c0252282a4b59de7896eAde9E28e9891B4f2

OKX Web3 DEX Router address:

0xF3dE3C0d654FDa23daD170f0f320a92172509127

SWFT bridge address:

0x92e929d8B2c8430BcAF4cD87654789578BB2b786

Bridge Destination Addresses:

TGzEDAa5XAmcTWVxSrZfmLqtRYnfAH6fih

TNmZkHDCdbq7f5DXr9Qsbyq26uDbbgUDNS

TTtVjeGux4Uaun8EJVWgEUYeCkdn8a2gM5

TCsAJrom3GBrtzToRgfi9rA5sA2cbbtqVB

TDBzuM9hAvBHP6yae417es9oqK66NEqVJ7

TUrhEAu6ufCvDtpKdDjJAZAGpNVDJoVVhg

TWNkDoiXcrBJM3yPQMEDMR8zU4hQZPPNjG

TYJvZuZAGDJQMgGAK4Sf8Gd3UcjCzokxAS

TG9WKX78JaVsstRAReEgvgt94RSSdwH7YR

Qbit owned wallets:

TYdJv19WaC992rhseXA4j27R5FM2dKVDqk **(the "Cregis Master Wallet")**

THGTenLmvqWycGLGtgRvX4wURiHQeDvNps ("THGTen")

ClassAction.org
