

1 Karl S. Kronenberger (CA Bar No. 226112)
2 **KRONENBERGER ROSENFELD, LLP**
3 548 Market Street, #85399
4 San Francisco, CA 94104
5 Telephone: (415) 955-1155
6 E-Mail: Karl@kr.law

7 David C. Silver (*pro hac vice forthcoming*)
8 Eric F. Rosenberg (*pro hac vice forthcoming*)
9 **SILVER MILLER**
10 4450 NW 126th Avenue - Suite 101
11 Coral Springs, Florida 33065
12 Telephone: (954) 516-6000
13 E-Mail: DSilver@SilverMillerLaw.com
14 E-Mail: ERosenberg@SilverMillerLaw.com

15 *Attorneys for Plaintiffs* [REDACTED]

16 **UNITED STATES DISTRICT COURT**
17 **FOR THE NORTHERN DISTRICT OF CALIFORNIA**

18 [REDACTED] an individual; and
19 [REDACTED] an individual;

20 Plaintiffs,

21 v.

22 THE CHARLES SCHWAB CORPORATION, a
23 Delaware corporation;
24 CHARLES SCHWAB BANK, SSB, a Texas-
25 chartered state savings bank;
26 BANK OF AMERICA, N.A., a national banking
27 association; and
28 UNCHAINED TRADING, LLC, a Texas limited
liability company;

Defendants.

Case No. 3:24-cv-07400

COMPLAINT FOR:

(1) FINANCIAL ELDER ABUSE
[Welf. & Inst. Code § 15600, *et seq.*]

(2) UNFAIR BUSINESS PRACTICES
[Bus. & Prof. Code § 17200]

(3) GROSS NEGLIGENCE

(4) VIOLATIONS OF SECTION 1693g OF
THE ELECTRONIC FUNDS TRANSFER
ACT [15 U.S.C. § 1693] AND SECTION
1005.6(B) OF FED. REG. E [12 C.F.R. §
1005.6]

(5) VIOLATIONS OF SECTION 1693c OF
THE ELECTRONIC FUNDS TRANSFER
ACT [15 U.S.C. § 1693] AND SECTION
1005.6 OF FED. REG. E [12 C.F.R. § 1005.6]

(6) VIOLATIONS OF SECTION 1693f OF
THE ELECTRONIC FUNDS TRANSFER
ACT [15 U.S.C. § 1693] AND SECTION
1005.11 OF FED. REG. E [12 C.F.R. §
1005.11]

DEMAND FOR JURY TRIAL

1 Plaintiffs [REDACTED] an individual (“[REDACTED] and [REDACTED] an individual
2 (“[REDACTED] (hereafter collectively referred to as “Plaintiffs”), by and through undersigned counsel,
3 sue Defendants THE CHARLES SCHWAB CORPORATION, a Delaware corporation; CHARLES
4 SCHWAB BANK, SSB, a Texas-chartered state savings bank; BANK OF AMERICA, N.A., a national
5 banking association; and UNCHAINED TRADING, LLC, a Texas limited liability company; for
6 damages and equitable relief. As grounds therefor, Plaintiffs allege the following:

7 **PRELIMINARY STATEMENT**

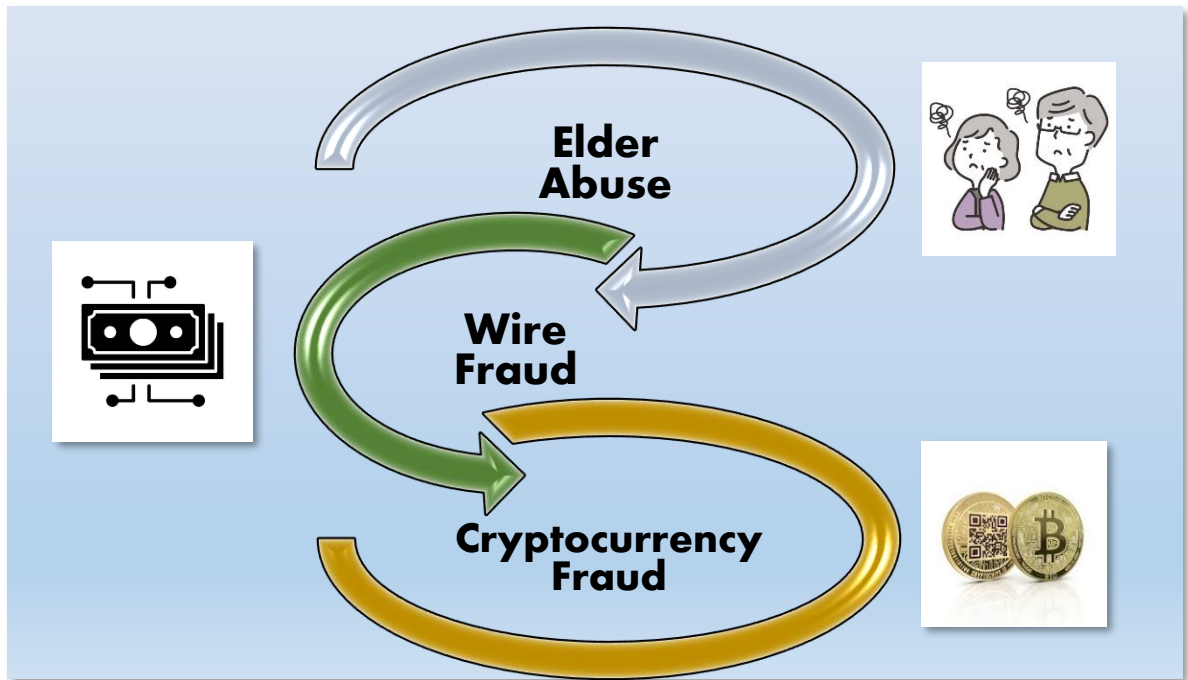
8 *“The world is a dangerous place -- not because of those who do evil,
9 but because of those who look on and do nothing.”*
10 -- Albert Einstein

11 1. This case arises from the calculated and devastating abuse of vulnerable elders,
12 committed by financial institutions that are required to -- but which failed in this instance to -- prevent
13 the very type of anomalous and suspicious fraudulent activity visited upon Plaintiffs.



14
15
16
17
18
19
20
21
22 2. What happened to Plaintiffs is happening to more and more victims of the unholy trinity
23 of elder abuse, wire fraud, and cryptocurrency fraud:

24 //
25 //
26 //
27 //
28 //



3. Through intricately scripted and fast-moving mechanisms, scammers dupe senior citizens into wiring large sums of money from their banking and investment accounts to cryptocurrency exchange accounts and private cryptocurrency wallets managed by the scammers, who then abscond with those funds.

4. As United States Senator Elizabeth Warren reported during a November 16, 2023 meeting of the U.S. Senate Special Committee on Aging:

Crypto is a favorite for those who are looking to defraud consumers. According to the FBI, in 2022, crypto scams were the leading cause of investment fraud in the United States. Using crypto, fraudsters stole a record \$2.5 billion from consumers.



But crypto fraud isn't hitting all consumers equally. Last year, we saw a 350% increase in crypto investment scams targeting seniors. That is the biggest spike among all age groups. That added up to more than \$1 billion that seniors lost in crypto scams. And because many victims don't report their experiences – as some

1 of you have noted – out of shame or fear, that \$1 billion figure is almost surely an
2 underestimate.¹

3 5. Those fraudulently-induced asset movements -- purportedly done to protect elders'
4 accounts -- however, would be, could be, and with the actual knowledge possessed by banks and money
5 transmitters should be halted in their tracks if the financial institutions through which they flow would
6 fulfill their statutory, regulatory, and common law obligations to monitor and prevent such illegal and
7 abusive activity.

8 6. As this lawsuit illustrates, financial institutions already have in their possession at the
9 time of these life-altering attacks on elders the actual knowledge and the tools to prevent this
10 catastrophic harm.

11 7. In the instant matter, and in countless other matters affecting senior citizens subjected
12 to financial exploitation, the financial institutions did not uphold their obligations and outright ignored
13 the actual knowledge they had of the abuse at hand -- all in the name of placing their own profits over
14 protecting the vulnerable clientele they serve.

15 8. As of the date of this filing, Plaintiffs have suffered grave economic harm for which
16 they seek compensatory and punitive damages as well as equitable relief to recover from the injuries
17 inflicted upon them.

18 9. As a result of the pattern of wrongful conduct of which they were made victims,
19 Plaintiffs seek damages in excess of the principal sum of Eighteen Million Five Hundred Thousand
20 Dollars (\$18,500,000.00), plus an unknown tax liability to be proven at trial, attorneys' fees and costs,
21 along with any other relief that this Court deems equitable and appropriate.

22 **THE PARTIES**

23 **PLAINTIFFS**

24 10. Plaintiff ██████████ ("████████" is a natural person domiciled in Los Angeles
25 County, California and is *sui juris*.

26 _____
27 ¹ "Modern Scams: How Scammers are Using Artificial Intelligence & How We Can Fight Back,"
28 U.S. Senate Special Committee on Aging, November 16, 2023,
<https://www.warren.senate.gov/newsroom/press-releases/at-hearing-senator-warren-highlights-dangers-of-crypto-scams-for-seniors-need-for-legislation>.

1 11. Plaintiff [REDACTED] (“[REDACTED]” is a natural person domiciled in Los Angeles
2 County, California and is *sui juris*.

3 12. At all times material hereto, [REDACTED] and [REDACTED] have been married to one another.

4 13. Additionally, at all times material hereto, THE CHARLES SCHWAB
5 CORPORATION, CHARLES SCHWAB BANK, SSB, and BANK OF AMERICA, N.A. held in their
6 records biographic information and personal identifying information denoting Plaintiffs’ age.
7 UNCHAINED TRADING, LLC likewise had such information in its records about [REDACTED]

8 **DEFENDANTS**

9 14. Defendant THE CHARLES SCHWAB CORPORATION is a financial services firm
10 based in the U.S. with operations worldwide that conducts business through its wholly-owned
11 subsidiaries. THE CHARLES SCHWAB CORPORATION is a Delaware corporation with its
12 headquarters at 3000 Schwab Way, Westlake, TX 76262. THE CHARLES SCHWAB
13 CORPORATION services accountholders, and thus conducts business, throughout the state of
14 California (including in this district) and the United States.

15 15. Defendant CHARLES SCHWAB BANK, SSB is a Texas-chartered state savings bank
16 with its headquarters at 3000 Schwab Way, Westlake, TX 76262. CHARLES SCHWAB BANK, SSB
17 is the banking subsidiary of Charles Schwab. CHARLES SCHWAB BANK, SSB services
18 accountholders, and thus conducts business, throughout the state of California (including in this district)
19 and the United States.

20 16. THE CHARLES SCHWAB CORPORATION and its wholly-owned subsidiary
21 CHARLES SCHWAB BANK, SSB are collectively referred to herein as “Charles Schwab.”

22 17. Defendant BANK OF AMERICA, N.A. (“BofA”) is a national banking association with
23 its headquarters and principal place of business in Charlotte, North Carolina. Among other things,
24 BofA is engaged in the business of providing retail banking services to consumers. BofA operates
25 banking centers, and thus conducts business, throughout the state of California (including in this
26 district) and the United States.

27 18. Defendant UNCHAINED TRADING, LLC (“UNCHAINED”) is a Texas limited
28 liability company with its principal place of business at 601 Congress Avenue - Suite 200, Austin, TX

1 78701-3214. UNCHAINED is a cryptocurrency exchange and licensed money transmitter subject to
2 numerous state and federal regulations, including the Bank Secrecy Act. Upon information and belief,
3 all members of the limited liability company reside in Texas. UNCHAINED services accountholders,
4 and thus conducts business, throughout the state of California (including in this district) and the United
5 States.

6 **OTHER LIABLE PERSONS/ENTITIES**

7 19. In addition to Defendants, there are likely other parties who may be liable to Plaintiffs,
8 but about whom Plaintiffs currently lack specific facts to permit them to name these persons or entities
9 as party defendants. By not naming such persons or entities at this time, Plaintiffs are not waiving their
10 right to amend this pleading to add such parties, should the facts warrant adding such parties.

11 **JURISDICTION AND VENUE**

12 20. This Court has original jurisdiction over the subject matter of this action pursuant to 28
13 U.S.C. § 1331, because the matter in controversy arises under the laws of the United States.

14 21. Additionally, the Court has supplemental jurisdiction over this action pursuant to 28
15 U.S.C. § 1367(a), involving claims that are so related to claims in the action within the Court's original
16 jurisdiction that they form part of the same case or controversy under Article III of the United States
17 Constitution.

18 22. The Court also has original subject-matter jurisdiction over this action pursuant to 28
19 U.S.C. § 1332, because there is complete diversity between the parties and the amount in controversy
20 exceeds \$75,000.00.

21 23. This Court has personal jurisdiction over Defendants because: (a) all Defendants are
22 operating, present, and/or doing business within this District, and (b) Defendants' breaches and
23 unlawful activity occurred within this District.

24 24. Venue is proper pursuant to 28 U.S.C. § 1391 in that at least one Defendant resides in
25 this judicial district and at least one Defendant is subject to the court's personal jurisdiction with respect
26 to this action. In light of the foregoing, this District is a proper venue in which to adjudicate this dispute.

27 //

28 //

1 **DIVISIONAL ASSIGNMENT**

2 25. Because a substantial part of the events which give rise to Plaintiffs' claims occurred
3 throughout the State of California, pursuant to Local Civil Rule 3-2(c), this action should be assigned
4 on a district-wide basis.

5 **GENERAL FACTUAL ALLEGATIONS**

6 **ELDER FINANCIAL ABUSE IS AS COMMON AS IT IS WIDE-SPREAD**

7 26. The exploitation and harm inflicted upon Plaintiffs is strikingly similar to a case
8 recently-filed in this jurisdiction highlighting the pervasive problem of financial institutions that fail to
9 uphold their duty to protect elders. *See, Rootenberg v. Charles Schwab & Co., Inc. and Charles Schwab*
10 *Bank, SSB*, U.S. District Court - Central District of California - Case No.: 2:24-cv-07645-JFW-RAO
11 (“*Rootenberg*”).

12 27. As *Rootenberg* set forth, elder financial abuse -- often called the “crime of the 21st
13 Century” -- is an epidemic with estimates of the annual economic losses as high as 37 billion dollars
14 per year.² Scams targeting their savings have proliferated over the last decade.³

15 28. Older adults are targets for financial exploitation due to their income and accumulated
16 life-long savings. Additionally, older adults are targeted due to their declining health, lack of
17 technological literacy, and higher likelihood to face isolation from family and friends during their
18 golden years.

19 29. Because threat actors rely on isolating their victims, institutions like Charles Schwab,
20 BofA, and UNCHAINED often serve as the only gatekeepers protecting vulnerable elders from
21 financial exploitation. Although elder abuse scams are often committed by unknown criminals, their
22 crimes rely on and benefit from the assistance of a bank or other financial institution -- in this case,
23 assistance and aid provided by agents and representatives of Charles Schwab, BofA, and
24

25 ² AARP & Princeton Survey Research Associates, AARP Research, Consumer Behavior, Experiences
26 and Attitudes: A Comparison by Age Groups (March 1999), available at Consumer Behavior,
Experiences and Attitudes: A Comparison by Age Groups (aarp.org).

27 ³ U.S. Treasury Financial Crimes Enforcement Network, Advisory on Elder Abuse, FinCEN Advisory,
28 FIN-2022-A002 (June 15, 2022), available at <https://www.fincen.gov/sites/default/files/advisory/2022-06-15/FinCEN%20Advisory%20Elder%20Financial%20Exploitation%20FINAL%20508.pdf>.

1 UNCHAINED, alongside those financial institutions' inadequate policies, procedures and controls or
2 those institutions' failure to properly implement policies, procedures, and controls.

3 30. [REDACTED] is an 84-year-old resident of Southern California, where he has lived for 21
4 years with his wife [REDACTED] (a 76-year-old) in a quiet suburban neighborhood.

5 31. Plaintiffs' stable, unassuming life was thrown upside down in mid-2024 when a series
6 of cataclysmic events sent them into financial peril.

7 32. The below timeline of events has been reconstructed to the best of Plaintiffs' and
8 undersigned counsel's ability based on documented records available at the time of this filing and based
9 on Plaintiffs' memory from a time period when Plaintiffs were under an extreme amount of stress and
10 duress.

11 CHRONOLOGY OF EVENTS

12 Pre-2024 to May 2024

13 33. Plaintiffs were legacy accountholders at TD Ameritrade, Inc., having held accounts at
14 TD Ameritrade for decades. They carefully crafted a sizeable investment portfolio valued at tens of
15 millions of dollars that belied their very modest lifestyle.

16 34. Plaintiffs are very private people, and the only people who were aware of Plaintiffs'
17 invested wealth were Plaintiffs themselves and the financial institution employees who maintained,
18 supervised, and were able to peer into Plaintiffs' portfolio.

19 35. In or about May 2024, Plaintiffs' investment holdings at TD Ameritrade transitioned to
20 accounts at Charles Schwab, as Charles Schwab had acquired TD Ameritrade in late-2020 and spent
21 nearly three-and-a-half years moving millions of TD customers onto the Charles Schwab platform.

22 36. While at TD Ameritrade, Plaintiffs' registered investment advisor was Joon Hyun Kim
23 (a/k/a Tony J. Kim), who himself transitioned from TD Ameritrade to Charles Schwab in May 2024.

24 37. Upon his May 2024 registration as a representative of Charles Schwab, Mr. Kim became
25 Plaintiffs' registered Charles Schwab financial consultant, bearing the title Vice President - Senior
26 Wealth Consultant - Schwab Private Wealth Services Certified Financial Planner.

27 38. Along with Mr. Kim, additional TD Ameritrade representatives transitioned to Charles
28 Schwab and brought with them knowledge of Plaintiffs' investment holdings and -- according to

1 recently-disclosed federal investigations -- a potential for exploiting elder investors like Plaintiffs.

2 39. Those investigations -- which led to settlements with the U.S. Department of Justice,
3 the Federal Reserve, the Office of the Comptroller of the Currency, and the U.S. Treasury Department's
4 Financial Crimes Enforcement Network (FinCEN) and required members of the TD Bank family of
5 companies to pay about \$3.1 billion in penalties -- found that for nearly a decade, TD Bank and its
6 affiliates had failed to put in place adequate controls to detect and prevent the flow of illicit money
7 through its accounts.

8 40. Among the more alarming discoveries revealed in those investigations was a finding
9 that TD employees had accepted tens of thousands of dollars' worth of bribes to foster a scheme to
10 launder more than \$650 million through TD Bank. In service to the fraudsters managing the scheme,
11 a widespread collection of TD employees readily ignored suspicious activity including large wire
12 transfers and questionable asset movement, refrained from reporting to regulators the crimes in which
13 they were partaking, and failed to utilize existing controls designed to prevent such illegal activity from
14 taking place.

15 41. Financial institution employees are trusted to monitor, investigate, and prevent financial
16 fraud when it occurs -- not to serve as the fuel to such engines of criminal enterprise.

17 42. When the trust imbued in financial institution employees is violated, not just the
18 institution itself but the customers of that institution are harmed.

19 43. While it is yet unknown whether Mr. Kim or any of the TD Ameritrade employees who
20 transitioned to Charles Schwab with knowledge of Plaintiffs' and their investment portfolio are
21 responsible for having directly violated the trust Plaintiffs had placed in them, it appears that a Charles
22 Schwab insider did just that.

23 **July 5-6, 2024**

24 44. On July 5, 2024, while monitoring Plaintiffs' accounts on the Charles Schwab website,
25 [REDACTED] received a pop-up message on his computer warning him that Plaintiffs' Charles Schwab
26 accounts had been compromised and were under attack from an unknown and unidentified source.

27 45. The pop-up message instructed [REDACTED] to contact Charles Schwab so that Charles
28 Schwab could assist Plaintiffs in securing their assets from the imminent threat presented by the account

1 compromise.

2 46. As Charles Schwab’s Head of Technology Risk Management Jeff Tricoli stated in a
3 June 14, 2024 fraud prevention Question-and-Answer chat session: *“It’s becoming increasingly difficult*
4 *for folks to distinguish between an authentic and a fraudulent message.”*⁴

5 47. On July 5, 2024, ██████ communicated with someone (phone number provided ***-
6 ***-3370) who identified and verified himself as a Charles Schwab representative by discussing with
7 ██████ Plaintiffs’ investment holdings at Charles Schwab and by providing confidential information
8 that only an insider at Charles Schwab would know about Plaintiffs and their investment holdings (the
9 “Schwab Threat Actor”).

10 48. At this initial stage of litigation, it is impossible for Plaintiffs to determine whether the
11 Schwab Threat Actor is a Charles Schwab insider, was working with Charles Schwab insiders to access
12 client information for large investment holders at Charles Schwab, or whether Charles Schwab or its
13 predecessor TD Ameritrade suffered a breach of confidential consumer data that has not been publicly
14 disclosed akin to the publicly-announced August 2023 Charles Schwab/TD Ameritrade customer data
15 breach that occurred as the two companies were transitioning millions of confidential client files from
16 TD Ameritrade to Charles Schwab.

17 49. What is known, however, is that the Schwab Threat Actor had an astonishingly accurate
18 amount of confidential information about Plaintiffs and their holdings at Charles Schwab which, upon
19 information and belief, would require inside access to Charles Schwab’s files and client databases.

20 50. As it has been publicly reported, the August 2023 customer data breach exposed
21 electronic files, Social Security numbers, financial account information, and other sensitive customer
22 data. Charles Schwab itself conceded that the data breach increased the risk of identity theft and other
23 fraudulent activities, such as those described hereinbelow.

24 51. Because Plaintiffs’ investment holdings have remained stable for many years, any
25 historical data released about the composition of their investments would have been as accurate in July
26 2024 as it would have been for several years prior.

27
28 ⁴ <https://www.schwab.com/learn/story/qa-future-cybercrime>.

1 52. On July 5-6, 2024, the Schwab Threat Actor and ██████ engaged in several phone calls
2 focused on Plaintiffs' investment holdings and what purportedly had to be done for Plaintiffs to
3 safeguard those holdings.

4 53. According to the Schwab Threat Actor, the first step Plaintiffs would have to undertake
5 would be to move all of their assets from the purportedly compromised Charles Schwab accounts to
6 external sources where they would be safe from dissipation.

7 54. Because Plaintiffs were long-time TD Ameritrade (now Charles Schwab)
8 accountholders and trusted that Charles Schwab was acting in good faith to best serve Plaintiffs'
9 interests, ██████ did as he was instructed to do by the Schwab Threat Actor to protect his and his
10 wife's sizeable and valuable Charles Schwab investment portfolio.

11 **July 8-9, 2024**

12 55. Having spoken on the phone several times ██████ the Schwab Threat Actor cultivated
13 with ██████ a relationship of trust, based on the Schwab Threat Actor's inside knowledge of Plaintiffs'
14 family accounts at Charles Schwab and the Schwab Threat Actor's repeated assurances that he was
15 acting to facilitate the transfer of Plaintiffs' assets to an alleged safe haven.

16 56. With the Schwab Threat Actor having demonstrated his ability to authenticate who he
17 was -- given his access to Plaintiffs' confidential and private Charles Schwab account information --
18 Plaintiffs allowed him the ability to remotely access their home computer.

19 57. It was only after the Schwab Threat Actor had verified his status with keenly precise
20 inside knowledge about Plaintiffs' Charles Schwab investment portfolio that ██████ -- starting on July
21 8, 2024 -- granted the Schwab Threat Actor the ability to remotely access Plaintiffs' home computer.

22 58. On July 8, 2024, the Schwab Threat Actor linked one of Plaintiffs' Charles Schwab
23 accounts to Plaintiffs' BofA account, which Plaintiffs had never previously done.

24 59. Later on July 8, 2024, the Schwab Threat Actor then submitted to Charles Schwab a
25 request to transfer funds from one of Plaintiffs' Charles Schwab accounts to their BofA account.

26 60. The transfers between Charles Schwab and BofA commenced with a transfer of
27 \$50,000.00 that was processed on July 9, 2024.

28

61. Prior to that transfer, Plaintiffs used their BofA account in a relatively limited manner; and the massive inflow of funds that was to follow this initial July 9, 2024 transfer -- including frequent and rapid electronic funds transfers in amounts exceeding \$1,000,000.00 each -- was wildly inconsistent with Plaintiffs' banking history at BofA.

62. On July 9, 2024, ██████ called Charles Schwab at 877-812-1817.

July 10, 2024

63. On July 10, 2024, the Schwab Threat Actor liquidated in one of Plaintiffs' Charles Schwab accounts over \$22,000,000.00 worth of several long-held stocks, *to wit*:

Stock:	Quantity:	Price (\$):	Charges/Interest (\$):	Amount (\$):
ADVANCED MICRO DEVICE IN (AMD)	2,500.0000	\$176.8850	\$12.71	\$442,199.79
APPLE INC (AAPL)	13,500.0000	\$228.4428	\$87.97	\$3,083,890.11
APPLIED MATERIALS (AMAT)	2,400.0000	\$250.7301	\$17.13	\$601,735.11
CISCO SYSTEMS INC (CSCO)	3,200.0000	\$45.8619	\$4.61	\$146,753.47
COMCAST CORP CLASS A (CMCSA)	2,300.0000	\$37.5150	\$2.78	\$86,281.72
CORNING INC (GLW)	4,200.0000	\$44.7901	\$5.93	\$188,112.49
EQT CORP (EQT)	1,500.0000	\$36.5900	\$1.78	\$54,883.22
NU SKIN ENTERPRISES CLASS A (NUS)	1,500.0000	\$9.8050	\$0.66	\$14,706.84
NVIDIA CORP (NVDA)	131,000.0000	\$130.1646	\$482.33	\$17,051,086.63
TERADYNE INCORPORATE (TER)	4,200.0000	\$153.5800	\$18.63	\$645,017.37
TOTAL:				\$22,314,666.75

64. The notable value and volume of those July 10, 2024 transactions placed Charles Schwab on actual notice of anomalous behavior in Plaintiffs' Charles Schwab accounts.

//

1 65. Charles Schwab utilizes internal behavioral account analysis and logical sequencing of
2 events in accounts to monitor accounts. Upon the \$22,000,000.00 sale of long-held stocks in one of
3 Plaintiffs' Charles Schwab accounts, multiple systems at Charles Schwab triggered alerts and actual
4 notices to different Charles Schwab departments about the large transactions; which required enhanced
5 surveillance, due diligence, Anti-Money Laundering (AML) surveillance, and Know Your Customer
6 (KYC) reporting because of the large transactions at issue.

7 66. Also on July 10, 2024, the Schwab Threat Actor -- utilizing the confidential information
8 he had about Plaintiffs and their holdings in their Charles Schwab accounts -- convinced ██████ that
9 a temporary account would need to be created at cryptocurrency exchange and licensed money
10 transmitting business UNCHAINED to protect Plaintiffs' assets.

11 67. Prior to July 10, 2024, Plaintiffs had never purchased, traded, or held any
12 cryptocurrency.

13 68. On July 10, 2024, an account was created for ██████ at UNCHAINED, the
14 cryptocurrency exchange with which Plaintiffs had no prior familiarity and no experience.

15 69. According to UNCHAINED's website, UNCHAINED utilizes enhanced security
16 measures that include a manual review of every single transaction through "*advanced corporate*
17 *controls.*"

18 The Unchained key

- 19 • Over 6 years of operational experience
20 securing billions of dollars worth of
21 bitcoin
- 22 • Every transaction manually reviewed with
23 advanced corporate controls
- 24 • SOC 1 & 2 certified

25 Our obsessive drive to ensure our key is safe
26 for hundreds of years is what defines the
27 Unchained key.



28 //

70. As UNCHAINED also states on its website:

Unchained is a financial institution as defined by the Bank Secrecy Act (BSA). As a financial institution, we are required to follow Anti-Money Laundering (AML) and Know Your Customer (KYC) practices. To comply, we must collect and verify sufficient information to form a reasonable belief that we know the true identity of the customer.

71. In less than one hour on July 10, 2024, UNCHAINED approved [REDACTED] account.

72. In the course of creating that account and acting to satisfy its Know Your Customer requirements, UNCHAINED obtained certain biographic information about [REDACTED] that included, among other things, his age.

July 11, 2024

73. On July 11, 2024, the Schwab Threat Actor liquidated over \$955,000.00 worth of additional long-held stock from one of Plaintiffs' Charles Schwab accounts:

Stock	Quantity	Price (\$)	Charges/Interest (\$)	Amount (\$)
A T & T INC (T)	800.0000	\$18.6800	\$0.55	\$14,943.45
ALPHABET INC. CLASS A (GOOGLE)	700.0000	\$191.2550	\$3.84	\$133,874.66
AMERN TOWER CORP REIT (AMT)	1,400.0000	\$194.5500	\$7.80	\$272,362.20
AVNET INC (AVT)	1,205.0000	\$51.4183	\$1.92	\$61,957.21
AWARE INC MASS (AWRE)	1,200.0000	\$1.8941	\$0.26	\$2,272.66
CHENIERE ENERGY INC (LNG)	1,300.0000	\$175.0000	\$6.54	\$227,493.46
FIRST AMER FINL (FAF)	900.0000	\$52.9300	\$1.47	\$47,635.53
JUNIPER NETWORKS INC (JNPR)	1,300.0000	\$36.9050	\$1.55	\$47,974.95
MICRON TECHNOLOGY (MU)	900.0000	\$135.2965	\$3.54	\$121,763.31
PFIZER INC (PFE)	900.0000	\$28.3603	\$0.86	\$25,523.41
TOTAL:				\$955,800.84

74. Just as with the stock liquidation the previous day, Charles Schwab had actual knowledge using its internal account and trade monitoring protocols that enhanced surveillance, due diligence, AML surveillance, and KYC reporting were required in the course of processing these transactions; and that any anomalous or suspicious activity had to be investigated and potentially halted.

75. Also on July 11, 2024, the Schwab Threat Actor created a link between Plaintiffs' BofA account and [REDACTED] new UNCHAINED account to fund the cryptocurrency account with fiat currency directly drawn from Plaintiffs' BofA account.

76. Additionally on July 11, 2024, the Schwab Threat Actor created a link between a second account Plaintiffs maintained at Charles Schwab -- linking that Charles Schwab account with Plaintiffs' BofA account to facilitate the flow of funds out of Charles Schwab and to BofA (and beyond).

77. With that newly-created Charles Schwab-BofA link in place, the Schwab Threat Actor electronically transferred \$100,000.00 from Plaintiffs' second Charles Schwab account to Plaintiffs' BofA account via a MoneyLink (*i.e.*, an Automated Clearing House ["ACH"]) transaction.

July 12, 2024

78. On July 12, 2024, the Schwab Threat Actor electronically transferred another \$100,000.00 from Plaintiffs' second Charles Schwab account to Plaintiffs' BofA account via a MoneyLink transaction.

July 13, 2024

79. On July 13, 2024, the Schwab Threat Actor created direct transfer links between Plaintiffs' Charles Schwab accounts and an account Plaintiffs held at Wells Fargo Bank, N.A. -- just as the Schwab Threat Actor had previously linked Plaintiffs' Charles Schwab accounts with their BofA account to facilitate the flow of funds away from Charles Schwab.

July 15, 2024

80. On July 15, 2024, the Schwab Threat Actor liquidated from one of Plaintiffs' jointly-held Charles Schwab accounts over \$2,250,000.00 worth of additional long-held stock.

Stock	Quantity	Price (\$)	Charges/Interest (\$)	Amount (\$)
ABBVIE INC (ABBV)	200.0000	\$170.7551	\$0.98	\$34,150.04

Stock	Quantity	Price (\$)	Charges/Interest (\$)	Amount (\$)
AKAMAI TECHNOLOGIES INC (AKAM)	3,300.0000	\$96.0750	\$9.36	\$317,038.14
AMERICAN FINL GROUP INC (AFG)	350.0000	\$125.9750	\$1.29	\$44,089.96
BANK OF AMERICA CORP (BAC)	1,400.0000	\$41.8650	\$1.86	\$58,609.14
CONOCOPHILLIPS (COP)	646.0000	\$113.0725	\$2.14	\$73,042.70
DELL TECHNOLOGIES INC CLASS C (DELL)	238.0000	\$140.0701	\$0.97	\$33,335.71
EDWARDS LIFESCIENCES (EW)	2,060.0000	\$92.3987	\$5.63	\$190,335.69
JABIL INC (JBL)	2,900.0000	\$115.3300	\$9.78	\$334,447.22
M & T BANK CORP (MTB)	500.0000	\$155.8700	\$2.25	\$77,932.75
MARATHON PETE CORP (MPC)	152.0000	\$164.9657	\$0.73	\$25,074.06
MARRIOTT INTL INC CLASS A (MAR)	900.0000	\$244.3801	\$6.26	\$219,935.83
MERCK & CO. INC. (MRK)	500.0000	\$128.1500	\$1.86	\$64,073.14
NISOURCE INC 00500 (NI)	1,035.0000	\$30.0801	\$1.04	\$31,131.86
RYDER SYSTEM INC (R)	700.0000	\$128.4933	\$2.62	\$89,942.69
SUPER MICRO COMPUTER (SMCI)	300.0000	\$914.5001	\$7.68	\$274,342.35
TE CONNECTIVITY LTD F (TEL)	340.0000	\$157.1000	\$1.54	\$53,412.46
TERADYNE INCORPORATE (TER)	400.0000	\$158.0600	\$1.83	\$63,222.17
VALERO ENERGY CORP (VLO)	1,152.0000	\$146.6150	\$4.89	\$168,895.59
WASTE MANAGEMENT INC (WM)	190.0000	\$214.2050	\$1.16	\$40,697.79

Stock	Quantity	Price (\$)	Charges/Interest (\$)	Amount (\$)
WELLS FARGO & CO (WFC)	1,007.0000	\$56.7849	\$1.76	\$57,180.63
TOTAL:				\$2,250,889.92

81. The stock holdings liquidated on July 15, 2024 were among the funds sent to Plaintiffs' account at BofA and later re-routed to UNCHAINED.

82. Additionally on July 15, 2024, the Schwab Threat Actor electronically transferred two \$100,000.00 payments each from Plaintiffs' Charles Schwab accounts to Plaintiffs' Wells Fargo Bank account via MoneyLink transactions: \$100,000.00 coming from one of Plaintiffs' Charles Schwab accounts, and a separate \$100,000.00 coming from another one of Plaintiffs' Charles Schwab accounts.

83. Charles Schwab authorized the two \$100,000.00 wire transfers without objection and without properly utilizing Enhanced Due Diligence.

84. Also on July 15, 2024, the Schwab Threat Actor electronically transmitted via a wire transfer another \$800,000.00 from one of Plaintiffs' Charles Schwab accounts to Plaintiffs' BofA account.

85. Charles Schwab likewise authorized the \$800,000.00 wire transfer without objection and without properly utilizing Enhanced Due Diligence.

July 16, 2024

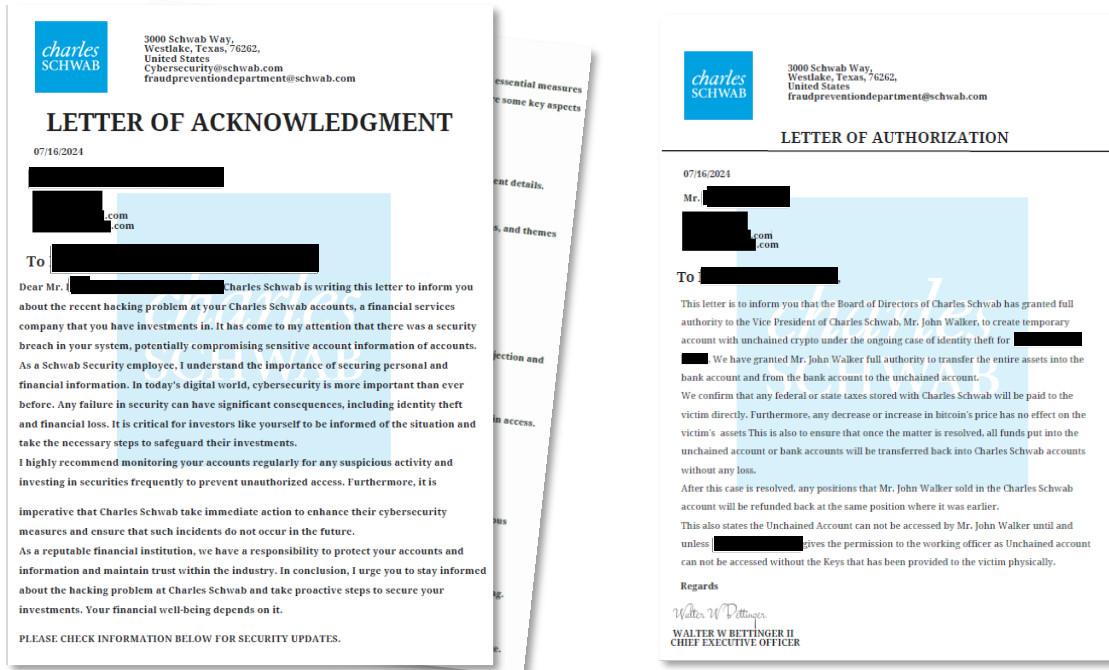
86. On July 16, 2024, the Schwab Threat Actor electronically transmitted via a wire transfer \$2,000,000.00 from one of Plaintiffs' Charles Schwab accounts to Plaintiffs' Wells Fargo Bank account.

87. Charles Schwab authorized the \$2,000,000.00 wire transfer without objection and without properly utilizing Enhanced Due Diligence.

88. Additionally on July 16, 2024, the Schwab Threat Actor electronically transmitted via a wire transfer \$2,000,000.00 from one of Plaintiffs' Charles Schwab accounts to Plaintiffs' BofA account.

89. Charles Schwab likewise authorized the second \$2,000,000.00 wire transfer without objection and without properly utilizing Enhanced Due Diligence.

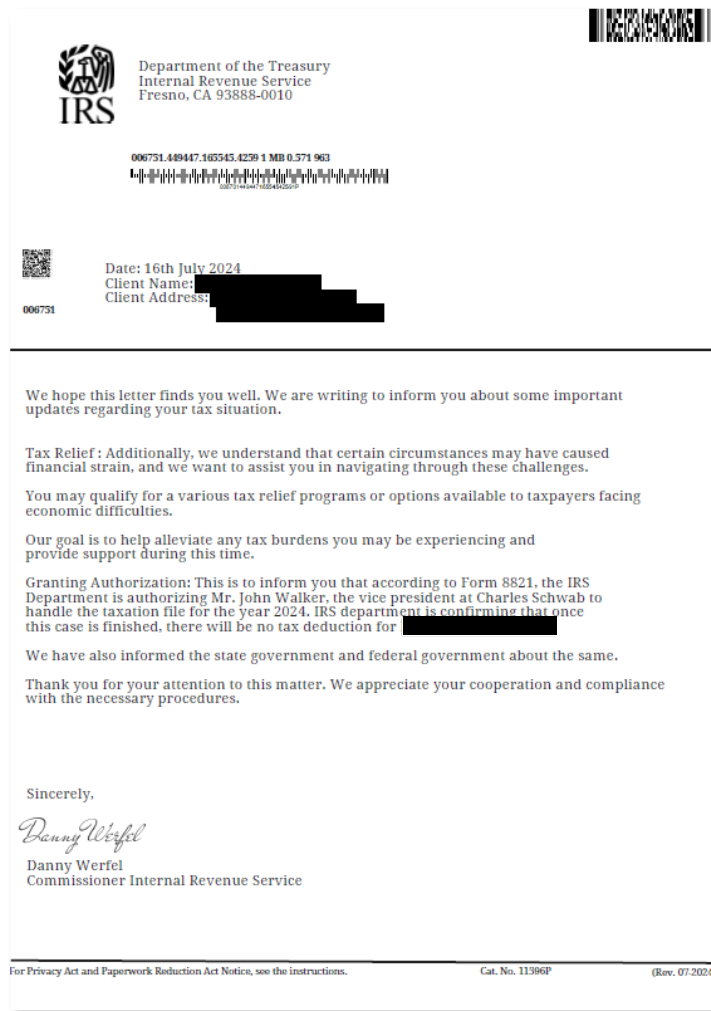
90. On July 16, 2024, the Schwab Threat Actor also electronically delivered to Plaintiffs a pair of letters purporting to be from Charles Schwab’s Fraud Prevention Department.



91. The letters -- which appear to be printed on Charles Schwab letterhead -- represented to Plaintiffs that Charles Schwab was diligently acting to protect Plaintiffs’ interests and to shield them from fraud. In furtherance of that effort, the letters stated that Charles Schwab Vice President John Walker had been authorized to oversee the transfer of Plaintiffs’ assets from Charles Schwab to bank accounts and then to UNCHAINED; and that *“once the matter is resolved, all funds put into the UNCHAINED account or bank accounts would be transferred back into Charles Schwab accounts without any loss.”*

92. As a corollary to those warning letters from Charles Schwab, the Schwab Threat Actor also delivered to Plaintiffs on or about July 16, 2024 a letter purporting to be from the Internal Revenue Service.

//
//
//
//
//



17 93. The letter -- which appears to be printed on IRS letterhead -- paralleled much of the
18 information in the July 16, 2024 Charles Schwab letters, again identifying Charles Schwab Vice
19 President John Walker as the person handling the matter for Plaintiffs.

20 **July 17, 2023**

21 94. On July 17, 2024, the Schwab Threat Actor electronically transmitted via a wire transfer
22 \$2,300,000.00 from one of Plaintiffs' Charles Schwab accounts to an account Plaintiffs maintained at
23 JPMorgan Chase Bank through a direct electronic link the Schwab Threat Actor had created.

24 95. Charles Schwab authorized the \$2,300,000.00 wire transfer without objection and
25 without properly utilizing Enhanced Due Diligence.

26 96. Also on July 17, 2024, the Schwab Threat Actor electronically transmitted via a wire
27 transfer \$3,000,000.00 from one of Plaintiffs' Charles Schwab accounts to Plaintiffs' Wells Fargo Bank
28 account.

1 97. Charles Schwab likewise authorized the \$3,000,000.00 wire transfer without objection
2 and without properly utilizing Enhanced Due Diligence.

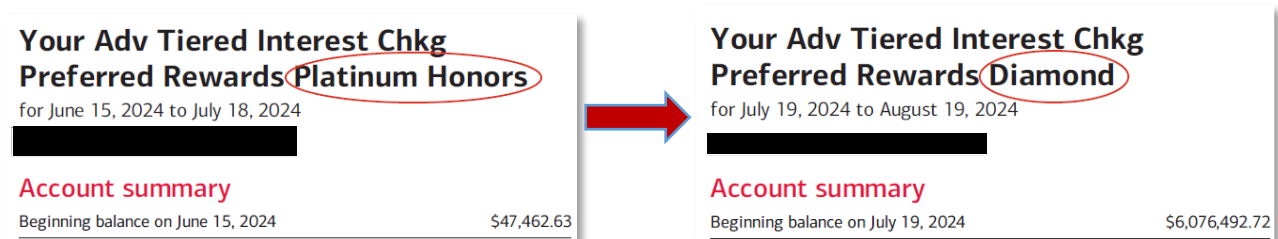
3 98. Additionally, commencing on July 17, 2024 and continuing for several days thereafter,
4 representatives at UNCHAINED (Connor Dolan and Jonathan Barrios) engaged in numerous
5 communications with the Schwab Threat Actor about onboarding ██████ as a client at UNCHAINED,
6 where the UNCHAINED representatives extended “concierge treatment” to best support the new
7 UNCHAINED account.

8 **July 18, 2024**

9 99. On July 18, 2024, the Schwab Threat Actor electronically transmitted via a wire transfer
10 \$3,000,000.00 from one of Plaintiffs’ Charles Schwab accounts to Plaintiffs’ BofA account.

11 100. Charles Schwab authorized the \$3,000,000.00 wire transfer to Plaintiffs’ BofA account
12 without objection and without properly utilizing Enhanced Due Diligence.

13 101. Additionally, on or about July 18, 2024 -- as BofA’s internal monitoring systems
14 recognized the increased flow of funds through Plaintiffs’ BofA account -- BofA upgraded Plaintiffs
15 from Platinum Honors account status to Diamond account status.



21 102. Therefore, as of July 18, 2024, BofA had actual notice and was actively monitoring
22 Plaintiffs’ account for anomalous behavior.

23 103. Rather than increase its scrutiny of the anomalous activity in Plaintiffs’ account, BofA
24 “rewarded” Plaintiffs upon seeing that their account had undergone an atypical transformation from
25 which BofA likely stood to profit.

26 104. The anomalous behavior at BofA during this time period provided actual notice to BofA
27 of the explicit elder financial exploitation as described in several BofA internal monitoring guidelines.
28

1 105. Based on this actual notice, this activity should have been flagged, stopped, segregated,
2 delayed, and marked for Enhanced Due Diligence based on regulator requirements, statutory
3 requirements, and BofA's own internal guidelines.

4 106. On information and belief, BofA employs independent third party service providers who
5 utilize artificial intelligence and machine learning to actively monitor the exact type of transactions as
6 described herein.

7 **July 22, 2024**

8 107. On July 22, 2024, the Schwab Threat Actor electronically transmitted via a wire transfer
9 \$4,000,000.00 from one of Plaintiffs' Charles Schwab accounts to Plaintiffs' BofA account.

10 108. Charles Schwab authorized the \$4,000,000.00 wire transfer without objection and
11 without properly utilizing Enhanced Due Diligence.

12 109. **Charles Schwab had clear and actual notice of the dramatically increasing amount
13 and frequency of the ACH and wire transfers being sent from Plaintiffs' Charles Schwab
14 accounts in a short period of time, yet Charles Schwab continued to authorize those transfers
15 without objection and without properly utilizing Enhanced Due Diligence.**

16 **After Plaintiffs' Charles Schwab Accounts Had Been Depleted**
17 **of Nearly \$18 Million,**
18 **The Bank Wires to Unchained Commenced**

19 **July 23, 2024**

20 110. On July 23, 2024, [REDACTED] went to the BofA branch office in Walnut, California where
21 he had previously engaged in limited banking services; and [REDACTED] requested that a wire transfer of
22 \$300,000.00 be sent to the newly-created UNCHAINED account.

23 111. Prior to July 23, 2024, Plaintiffs had consistently only performed limited services at
24 BofA.

25 112. Prior to July 23, 2024, Plaintiffs had never sent any wire transfers and had never engaged
26 in banking transactions on the level that would flow through Plaintiffs' BofA accounts over the next
27 several days and weeks.

28 113. [REDACTED] met that day with BofA bankers -- discussing with them the nature and purpose
of the requested wire transfer.

1 114. [REDACTED] specifically advised the BofA bankers that he was having a security issue with
2 his Charles Schwab account and that he was moving his assets to a cryptocurrency exchange to protect
3 his assets, as instructed by Charles Schwab.

4 115. After discussing the matter with [REDACTED] BofA authorized the wire transfer without
5 objection and without properly utilizing Enhanced Due Diligence.

6 116. On July 23, 2024, UNCHAINED confirmed in an e-mail sent to the e-mail address
7 registered for [REDACTED] UNCHAINED account that it had received the \$300,000.00 deposit into [REDACTED]
8 [REDACTED] UNCHAINED account. UNCHAINED also wrote that to smoothly facilitate future wire transfers
9 of funds into the UNCHAINED account: *“Please add any bank accounts from which you would like to
10 wire money, once bank is approved, you may send wires from connected account. Your connected bank
11 accounts are how we know the wire belongs to you -- its [sic.] a very important step.”*

12 117. After receiving the \$300,000.00 wire transfer, UNCHAINED processed a July 23, 2024
13 transaction for the purchase of cryptocurrency in [REDACTED] UNCHAINED account in the amount of
14 \$300,000.00.

15 118. Within approximately 72 hours of its purchase, the newly-purchased \$300,000.00 worth
16 of cryptocurrency was withdrawn from [REDACTED] UNCHAINED account and sent to a cryptocurrency
17 address (the “****260zma Address”) believed to be maintained by the Schwab Threat Actor.

18 **July 24, 2024**

19 119. On July 24, 2024, the Schwab Threat Actor (posing as [REDACTED] e-mailed UNCHAINED
20 and asked to transfer more money into [REDACTED] UNCHAINED account. UNCHAINED responded
21 that an accountholder can only have one active trade order at a time and that wired funds would sit in
22 a cash balance with UNCHAINED until the current, active trade settles and the BTC purchased is
23 deposited into the accountholder’s account.

24 120. UNCHAINED asked no questions as to why there was such urgency to engage in trading
25 in the newly-created account for [REDACTED] at UNCHAINED.

26 121. Also on July 24, 2024, [REDACTED] received an electronic mail message from Tony Kim,
27 his trusted financial consultant at TD Ameritrade and subsequently at Charles Schwab, stating that
28 Charles Schwab’s Tax, Trust and Estates strategists are available to consult about any tax or estate

1 planning questions ██████ may have.

2 122. The message from Mr. Kim at Charles Schwab was internally triggered by monitoring
3 software at Charles Schwab and demonstrates that Charles Schwab had actual knowledge of the
4 anomalous behavior/activity in Plaintiffs' account.

5 123. **Rather that act as required by the BSA to protect Plaintiffs, though, Charles**
6 **Schwab simply sought to offer Plaintiffs additional account services at Charles Schwab.**

7 124. Additionally, on July 24, 2024, ██████ went to the Wells Fargo Bank branch office in
8 Walnut, California where he had previously engaged in banking services; told the Wells Fargo Bank
9 representatives the same thing he had told BofA; and requested that a wire transfer of \$3,000,000.00
10 be sent to the newly-created UNCHAINED account.

11 125. After communicating with ██████ multiple times and considering the anomalous
12 request, Wells Fargo refused to process the \$3,000,000.00 wire transfer.

13 **August 1, 2024**

14 126. On August 1, 2024, ██████ went back to the BofA branch office in Walnut, California
15 which had authorized a previous \$300,000.00 wire transfer to UNCHAINED a week earlier, and ██████
16 ██████ requested that a wire transfer of \$700,000.00 be sent to the UNCHAINED account.

17 127. Again, ██████ met that day with BofA bankers -- discussing with them the nature and
18 purpose of the requested wire transfer.

19 128. Consistent with his July 23, 2024 meeting at that same BofA branch, ██████ provided
20 the BofA representatives the same information about account security issues at Charles Schwab and
21 his need to move all of his assets to UNCHAINED for protection.

22 129. Upon evaluating the anomalous and suspicious request, the BofA representatives in
23 Walnut, California refused to process the \$700,000.00 wire transfer.

24 130. BofA has internal policies and procedures that require annotating client accounts and
25 reporting to proper authorities/regulatory agencies any suspicious activity attempted or engaged in by
26 BofA customers. Such notations prevent illicit activity and prevent elder customers susceptible to fraud
27 from being manipulated in search of permissive bankers who are willing to ignore or refuse to act upon
28 such warning signs of fraudulent activity.

1 131. Upon information and belief, BofA’s policies and procedures require that its bankers
2 memorialize in writing their reasons for refusing to authorize the \$700,000.00 wire request.

3 132. **Notwithstanding those policies and procedures, BofA -- as noted below -- ignored**
4 **its own internal warnings of suspicious activity and proceeded to authorize numerous more**
5 **fraudulently-procured wire transfers from Plaintiffs’ BofA account to UNCHAINED over the**
6 **ensuing weeks.**

7 133. On August 1, 2024, the Schwab Threat Actor (again posing as ██████ e-mailed
8 UNCHAINED the following:

9 Hello,

10 I have been trying to make deposits to my Unchained account and every bank I tried to make the wire
11 transfer with they all said that it seems to be very risky, and we can't do the wire transfer and all the wire
12 transfers i have made so far have been denied.

13 Banks including -
14 Bank of America
15 Wells Fargo
16 chase
17 Charles Schwab Checking

18 I would like to ask if there is any other way that we can deposit the money into my unchained account.

Wires OUT	
Charles Schwab	– \$29,550,000
BofA	– \$22,000,000
Wells Fargo	– STOPPED WIRE FOR FRAUD
Chase	– STOPPED WIRE FOR FRAUD

19 134. UNCHAINED responded to the Schwab Threat Actor’s message a few hours later by
20 acknowledging that UNCHAINED had received the wire transfer from BofA the prior week and
21 suggested that ██████ (actually the Schwab Threat Actor) try BofA again.

22 135. The Schwab Threat Actor then responded thusly on August 1, 2024:

23 I did go to my Bank of America branch again but then they say it is too risky and we cannot do the wire
24 transfer so my concern is can you provide me with some document that can help me with my Bank to make
25 the wire transfer

26 136. In the face of being advised that the initiating banks considered wire transfers to
27 UNCHAINED to be “too risky” -- and with the actual knowledge that the banks were rejecting the
28 requested wire transfers purportedly coming from 84-year-old ██████ to UNCHAINED --
UNCHAINED remain undeterred and suggested in a response e-mail on the afternoon of August 1, 2024
that ██████ (actually the Schwab Threat Actor) try the initiating banks again and support the purported
legitimacy of transferring money to UNCHAINED by explaining to the banks that UNCHAINED is a
“registered money service” that is “highly regulated and subject to many of the same requirements and

1 *standards as banks.”*

2 **August 2, 2024**

3 137. On August 2, 2024, [REDACTED] -- at the direction of the Schwab Threat Actor -- went to a
4 BofA branch office in Diamond Bar, California where he had not previously engaged in banking
5 services; and [REDACTED] requested that a wire transfer of \$700,000.00 -- the same amount that had been
6 rejected by the Walnut, California BofA branch the previous day -- be sent to the UNCHAINED
7 account.

8 138. As he had previously done at the Walnut, California BofA bank branch, [REDACTED] met
9 with BofA bankers and discussed the nature and purpose of the requested wire transfer -- explaining to
10 the BofA representatives the Charles Schwab account security issues of which he had been told and his
11 need to move all of his assets to UNCHAINED for protection, as instructed by Charles Schwab.

12 139. **Despite an identical wire transfer request having been rejected by a different BofA**
13 **branch the previous day, the BofA branch in Diamond Bar, California authorized the**
14 **\$700,000.00 wire transfer without objection and without properly utilizing Enhanced Due**
15 **Diligence.**

16 140. BofA policies and procedures, as well as regulatory requirements, are designed to
17 prevent precisely this type of activity: a suspicious, large dollar-figure wire transfer request by an
18 elderly customer being rejected by one bank branch and then being approved by a different bank branch
19 the following day.

20 141. In this instance, BofA failed to satisfy such policies and procedures and its duty of care
21 to Plaintiffs.

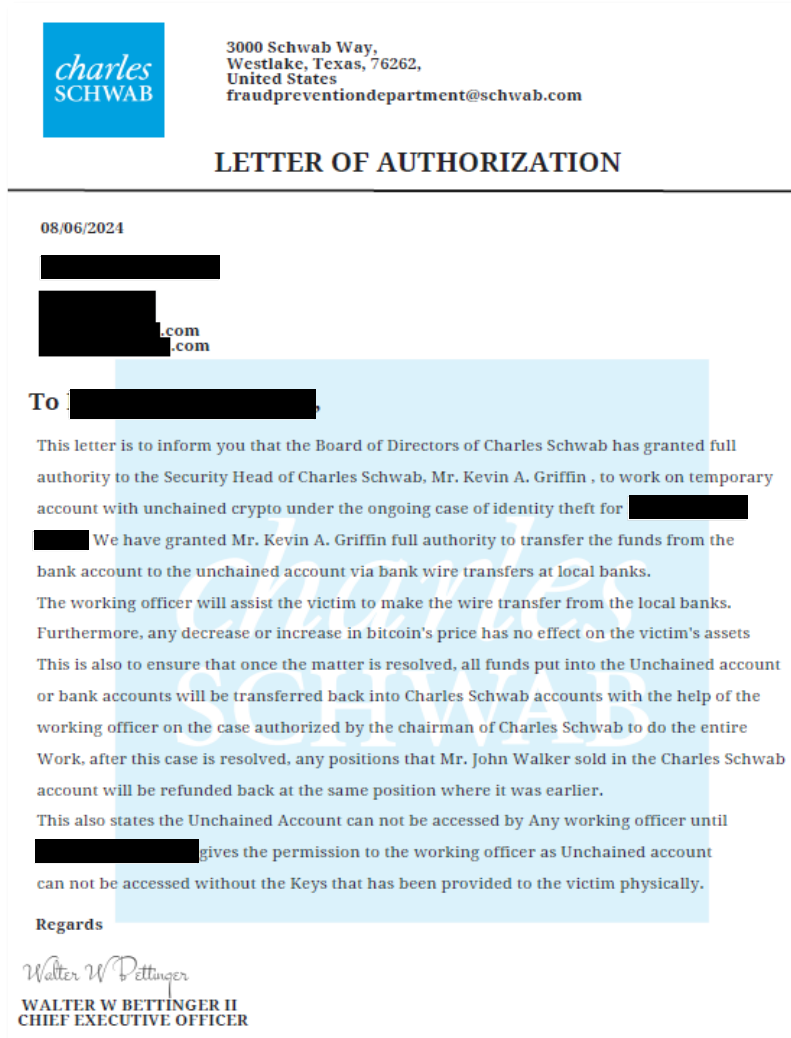
22 142. After receiving the \$700,000.00 wire transfer, UNCHAINED e-mailed [REDACTED] on
23 August 2, 2024 to confirm its receipt of the wire transfer and then processed an August 2, 2024
24 transaction for the purchase of cryptocurrency in [REDACTED] UNCHAINED account in the amount of
25 \$700,000.00.

26 143. Within approximately four days of its purchase, the newly-purchased \$700,000.00
27 worth of cryptocurrency was withdrawn from [REDACTED] UNCHAINED account and sent to the
28 ***260zma Address, which is believed to be maintained by the Schwab Threat Actor.

August 6, 2024

144. On August 6, 2024, the Schwab Threat Actor electronically delivered to [REDACTED] another letter -- this one purporting to be from Charles Schwab's Fraud Prevention Department.

145. The letter -- which appears to be printed on Charles Schwab letterhead -- stated the following:



146. [REDACTED] believed the letter to be legitimate and continued to follow the instructions given to him by the Schwab Threat Actor.

147. On August 6, 2024, [REDACTED] again went to the BofA branch office in Diamond Bar, California; and [REDACTED] requested that a wire transfer of \$2,000,000.00 be sent to the UNCHAINED account.

1 148. ██████ met that day with a BofA banker and discussed the nature and purpose of the
2 requested wire transfer -- again explaining to the BofA representative the Charles Schwab account
3 security issues of which he had been told and his need to move all of his assets to UNCHAINED for
4 protection, as instructed by Charles Schwab.

5 149. BofA had clear and actual knowledge of the rejected wire transfer at a BofA branch
6 earlier that week as well as the increasing amount of the wire transfers being sent from Plaintiffs' BofA
7 account in a short period of time.

8 150. BofA authorized the \$2,000,000.00 wire transfer without objection and without properly
9 utilizing Enhanced Due Diligence.

10 151. After receiving the \$2,000,000.00 wire transfer, UNCHAINED e-mailed ██████ on
11 August 6, 2024 to confirm its receipt of the wire transfer and then processed an August 6, 2024
12 transaction for the purchase of cryptocurrency in ██████ UNCHAINED account in the amount of
13 \$2,000,000.00.

14 152. Within approximately 24 hours of its purchase, the newly-purchased \$2,000,000.00
15 worth of cryptocurrency was withdrawn from ██████ UNCHAINED account and sent to the
16 ***260zma Address, which is believed to be maintained by the Schwab Threat Actor.

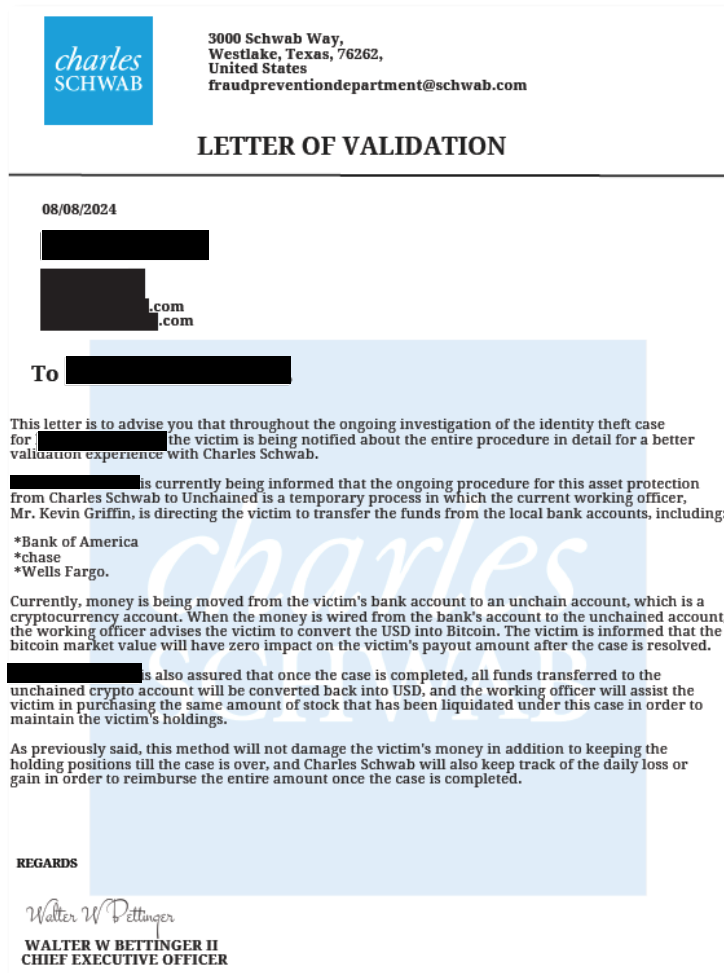
17 **August 8, 2024**

18 153. On August 8, 2024, the Schwab Threat Actor electronically delivered to ██████ another
19 letter purporting to be from Charles Schwab's Fraud Prevention Department.

20 154. The letter -- which appears to be printed on Charles Schwab letterhead -- stated the
21 following:

22 //
23 //
24 //
25 //
26 //
27 //
28 //

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28



155. [Redacted] believed the letter to be legitimate and continued to follow the instructions given to him by the Schwab Threat Actor.

August 9-10, 2024

156. On August 9, 2024, [Redacted] again went to the BofA branch office in Diamond Bar, California; and [Redacted] requested that a wire transfer of \$3,500,000.00 be sent to the UNCHAINED account.

157. As on previous trips to that bank branch, [Redacted] met that day with a BofA banker and discussed the nature and purpose of the requested wire transfer -- again explaining to the BofA representative the Charles Schwab account security issues of which he had been told and his need to move all of his assets to UNCHAINED for protection, as instructed by Charles Schwab.

158. BofA authorized the \$3,500,000.00 wire transfer without objection and without properly utilizing Enhanced Due Diligence.

1 159. BofA had clear and actual knowledge of the earlier-rejected wire transfer and the
2 increasing amount of the wire transfers being sent from Plaintiffs' BofA account in a short period of
3 time.

4 160. After receiving the \$3,500,000.00 wire transfer, UNCHAINED e-mailed [REDACTED] on
5 August 9, 2024 to confirm its receipt of the wire transfer, to thank him for his business, and to express
6 its happiness that UNCHAINED has been able to help [REDACTED] through the onboarding process and
7 through the settlement of each transaction.

8 161. UNCHAINED also stated in its August 9, 2024 e-mail to [REDACTED] that UNCHAINED
9 was willing to reduce its private client trading fee and -- due to his recent activity -- to waive \$1,000 of
10 the annual cost of doing business at UNCHAINED.

11 162. **Rather that act to protect [REDACTED] UNCHAINED -- seeing the rapid movement of**
12 **assets into and out of [REDACTED] account -- sought to entice [REDACTED] on additional business at**
13 **UNCHAINED.**

14 163. After receiving the \$3,500,000.00 wire transfer, processed an August 10, 2024
15 transaction for the purchase of cryptocurrency in [REDACTED] UNCHAINED account in the amount of
16 \$3,500,000.00.

17 164. Within approximately four days of its purchase, the newly-purchased \$3,500,000.00
18 worth of cryptocurrency was withdrawn from [REDACTED] UNCHAINED account and sent to the
19 ***260zma Address, which is believed to be maintained by the Schwab Threat Actor.

20 **August 13-14, 2024**

21 165. On August 13, 2024, [REDACTED] again went to the BofA branch office in Diamond Bar,
22 California; and [REDACTED] requested that a wire transfer of \$3,500,000.00 be sent to the UNCHAINED
23 account.

24 166. [REDACTED] met that day with a BofA banker and discussed the nature and purpose of the
25 requested wire transfer -- again explaining to the BofA representative the Charles Schwab account
26 security issues of which he had been told and his need to move all of his assets to UNCHAINED for
27 protection, as instructed by Charles Schwab.

28 167. BofA authorized the \$3,500,000.00 wire transfer without objection and without properly

1 utilizing Enhanced Due Diligence.

2 168. After receiving the \$3,500,000.00 wire transfer, UNCHAINED e-mailed [REDACTED] on
3 August 13, 2024 to confirm its receipt of the wire transfer and then processed an August 14, 2024
4 transaction for the purchase of cryptocurrency in [REDACTED] UNCHAINED account in the amount of
5 \$3,500,000.00.

6 169. Within approximately 48 hours of its purchase, the newly-purchased \$3,500,000.00
7 worth of cryptocurrency was withdrawn from [REDACTED] UNCHAINED account and sent to the
8 ***260zma Address, which is believed to be maintained by the Schwab Threat Actor.

9 **August 22-23, 2024**

10 170. On August 22, 2024, the Schwab Threat Actor electronically transmitted via a wire
11 transfer \$5,000,000.00 from one of Plaintiffs' Charles Schwab accounts to Plaintiffs' BofA account.

12 171. Charles Schwab authorized the \$5,000,000.00 wire transfer without objection and
13 without properly utilizing Enhanced Due Diligence.

14 172. On August 23, 2024, [REDACTED] again went to the BofA branch office in Diamond Bar,
15 California; and [REDACTED] requested that a wire transfer of \$5,000,000.00 be sent to the UNCHAINED
16 account.

17 173. [REDACTED] met that day with a BofA banker and discussed the nature and purpose of the
18 requested wire transfer -- again explaining to the BofA representative the Charles Schwab account
19 security issues of which he had been told and his need to move all of his assets to UNCHAINED for
20 protection, as instructed by Charles Schwab.

21 174. BofA authorized the \$5,000,000.00 wire transfer without objection and without properly
22 utilizing Enhanced Due Diligence.

23 175. **In the span of just three short weeks (August 2, 2024 - August 23, 2024), the wire**
24 **transfers from Plaintiffs' BofA account -- from which no wire transfers had ever previously been**
25 **sent -- had increased from \$700,000.00 to \$2,000,000.00 to \$3,500,000.00 to \$5,000,000.00.**

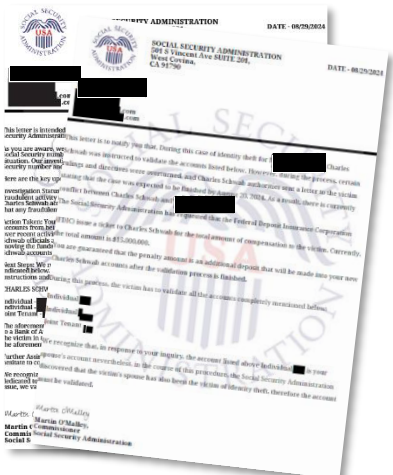
26 176. **BofA had clear and actual knowledge of the increasing amount of the wire**
27 **transfers being sent from Plaintiffs' BofA account in a short period of time, yet BofA continued**
28 **to authorize them.**

1 177. After receiving the \$5,000,000.00 wire transfer, UNCHAINED e-mailed [REDACTED] on
2 August 23, 2024 to confirm its receipt of the wire transfer and then processed an August 26, 2024
3 transaction for the purchase of cryptocurrency in [REDACTED] UNCHAINED account in the amount of
4 \$5,000,000.00.

5 178. Within approximately five days of its purchase, the newly-purchased \$5,000,000.00
6 worth of cryptocurrency was withdrawn from [REDACTED] UNCHAINED account and sent to the
7 ***260zma Address, which is believed to be maintained by the Schwab Threat Actor.

8 **August 29-September 7, 2024**

9 179. [REDACTED] also received from the Schwab Threat Actor a series of letters in or about late-
10 August/early-September 2024 purporting to be from the Social Security Administration and Charles
11 Schwab.



12
13
14
15
16
17
18
19
20 180. The letters represented to [REDACTED] that his Social Security Number had been
21 compromised as had his Charles Schwab accounts, which the letters instructed [REDACTED] had to be
22 liquidated and moved to his UNCHAINED account as a way of “safeguarding his assets.” According
23 to the letters, all of [REDACTED] assets (no less than \$15,000,000.00 at that point) would be returned to
24 him “after the validation process is finished” and requested that [REDACTED] “assume responsibility and
25 execute all activities, including liquidation and bank transfers.”

26 **September 10, 2024**

27 181. On September 10, 2024, [REDACTED] electronically transferred from one of Plaintiffs’
28 Charles Schwab accounts to their BofA account \$7,000,000.00.

1 182. Charles Schwab authorized the \$7,000,000.00 wire transfer without objection and
2 without properly utilizing Enhanced Due Diligence.

3 **September 11, 2024**

4 183. On September 11, 2024, [REDACTED] again went to the BofA branch office in Diamond Bar,
5 California; and [REDACTED] requested that a wire transfer of \$3,500,000.00 be sent to the UNCHAINED
6 account.

7 184. [REDACTED] met that day with a BofA banker and discussed the nature and purpose of the
8 requested wire transfer -- again explaining to the BofA representative the Charles Schwab account
9 security issues of which he had been told and his need to move all of his assets to UNCHAINED for
10 protection, as instructed by Charles Schwab.

11 185. BofA authorized the \$3,500,000.00 wire transfer without objection and without properly
12 utilizing Enhanced Due Diligence.

13 186. After receiving the \$3,500,000.00 wire transfer, UNCHAINED e-mailed [REDACTED] on
14 September 11, 2024 to confirm its receipt of the wire transfer and then processed a September 12, 2024
15 transaction for the purchase of cryptocurrency in [REDACTED] UNCHAINED account in the amount of
16 \$3,500,000.00.

17 187. Within approximately 24 hours of its purchase, the newly-purchased \$3,500,000.00
18 worth of cryptocurrency was withdrawn from [REDACTED] UNCHAINED account and sent to the
19 ***260zma Address, which is believed to be maintained by the Schwab Threat Actor.

20 **September 13-16, 2024**

21 188. On September 13, 2024, [REDACTED] again went to the BofA branch office in Diamond Bar,
22 California; and [REDACTED] requested that a wire transfer of \$3,500,000.00 be sent to the UNCHAINED
23 account.

24 189. [REDACTED] met that day with a BofA banker and discussed the nature and purpose of the
25 requested wire transfer -- once more explaining to the BofA representative the Charles Schwab account
26 security issues of which he had been told and his need to move all of his assets to UNCHAINED for
27 protection, as instructed by Charles Schwab.

28 190. BofA authorized the \$3,500,000.00 wire transfer without objection and without properly

1 utilizing Enhanced Due Diligence.

2 191. After receiving the \$3,500,000.00 wire transfer, UNCHAINED e-mailed [REDACTED] on
3 September 13, 2024 to confirm its receipt of the wire transfer; however, a subsequent cryptocurrency
4 transaction in the ensuing days was not processed.

5 **September 16, 2024**

6 192. Upon information and belief, it was on or about September 16, 2024 that the U.S.
7 Federal Bureau of Investigation intervened and began providing notice to involved parties -- including
8 Plaintiffs, Charles Schwab, BofA, and UNCHAINED -- that Plaintiffs had been subjected to a
9 sophisticated and illegal elder fraud scheme.

10 193. Before Plaintiffs discovered that they had been the victims of an elaborate scam, though,
11 the Schwab Threat Actor -- on September 16, 2024 -- was able to liquidate from one of Plaintiffs'
12 Charles Schwab accounts over \$11 million in NVIDIA stock.

13 194. The September 16, 2024 sale of the NVIDIA stock was an unauthorized transaction and
14 caused Plaintiffs a multi-million dollar tax liability they did not bring upon themselves.

15 195. On September 16, 2024, [REDACTED] received from UNCHAINED an e-mail informing [REDACTED]
16 [REDACTED] in an abrupt fashion that his UNCHAINED account was being closed and that any cash balance in
17 the account would be returned to [REDACTED]

18 196. In part, the message from UNCHAINED stated:

19 To whom it may concern,
20 This email provides notice that Unchained has decided to end its relationship and close your account. This
21 decision is final and cannot be reversed.
22 Effective immediately, Unchained will close any active accounts and return any cash balance. We understand
23 that this news may come as a surprise, and we want to ensure a smooth transition. To facilitate the process,
24 we kindly ask you to take the following steps:


25 **September 18, 2024**

26 197. On September 18, 2024, UNCHAINED returned to Plaintiffs' BofA account the
27 \$3,500,000.00 cash balance that was deposited into the UNCHAINED account a few days earlier.

28 //


THE FLOW OF FUNDS STOLEN FROM PLAINTIFFS

198. The following chart summarizes the fraudulently-procured and inappropriately authorized electronic funds transfers that -- in ever-increasing amounts in a short amount of time -- were sent from Plaintiffs' Charles Schwab accounts to Plaintiffs' bank accounts:


Charles Schwab Accounts			
Date	Transaction Reference Number	Recipient	Amount
07/09/2024	[MoneyLink transaction]	Bank of America	\$50,000.00
07/11/2024	[MoneyLink transaction]	Bank of America	\$100,000.00
07/12/2024	[MoneyLink transaction]	Bank of America	\$100,000.00
07/15/2024	[MoneyLink transaction]	Wells Fargo Bank	\$100,000.00
07/15/2024	[MoneyLink transaction]	Wells Fargo Bank	\$100,000.00
07/15/2024	071511B7033R023663	Bank of America	\$800,000.00
07/16/2024	2024071600048608	Wells Fargo Bank	\$2,000,000.00
07/16/2024	071611B7031R017042	Bank of America	\$2,000,000.00
07/17/2024	071711B7032R000298	JPMorgan Chase Bank	\$2,300,000.00
07/17/2024	2024071700141010	Wells Fargo Bank	\$3,000,000.00
07/18/2024	071811B7033R012486	Bank of America	\$3,000,000.00
07/22/2024	072211B7031R014968	Bank of America	\$4,000,000.00
08/22/2024	Case ID: WI-113025923	Bank of America	\$5,000,000.00
09/10/2024	091011B7031R020529	Bank of America	\$7,000,000.00
TOTAL			\$29,550,000.00


199. The following chart summarizes the fraudulently-procured and inappropriately authorized wire transfers from Plaintiffs' BofA account to UNCHAINED -- in ever-increasing amounts in a short amount of time -- only the last of which was returned to Plaintiffs:

//
//
//
//

Bank of America Account			
Date	Transaction Reference Number	Recipient	Amount
07/23/2024	2024072300477807	Unchained Trading LLC	\$300,000.00
08/02/2024	2024080200556744	Unchained Trading LLC	\$700,000.00
08/06/2024	2024080600460426	Unchained Trading LLC	\$2,000,000.00
08/09/2024	2024080900504993	Unchained Trading LLC	\$3,500,000.00
08/13/2024	2024081300428585	Unchained Trading LLC	\$3,500,000.00
08/23/2024	2024082300540694	Unchained Trading LLC	\$5,000,000.00
09/11/2024	2024091100477203	Unchained Trading LLC	\$3,500,000.00
09/13/2024	2024091300497252	Unchained Trading LLC	\$3,500,000.00
TOTAL			\$22,000,000.00

200. Additionally, the following chart shows the rapid succession of the flow of funds into the account at UNCHAINED, conversion of those funds into cryptocurrency, and the swift withdrawal of those cryptocurrency assets out of the UNCHAINED account within days if not hours of their arrival -- all in a manner bearing the hallmarks of suspicious activity that UNCHAINED was obligated to investigate, report, and halt:

Unchained Account			
Transaction Type	Date/Time	BTC	USD Value
Trade Executed	July 23, 2024, 4:17 PM	4.5045337	\$300,000.00
Deposit	July 24, 2024, 11:30 AM	4.5045337	\$300,000.00
Trade Settled	July 24, 2024, 2:53 PM	4.5045337	\$300,000.00
Withdrawal	July 26, 2024, 9:29 AM	4.5045337	\$300,000.00
Trade Executed	August 2, 2024, 5:22 PM	11.21639738	\$700,000.00
Deposit	August 5, 2024, 2:52 PM	11.21639738	\$700,000.00
Trade Settled	August 5, 2024, 4:51 PM	11.21639738	\$700,000.00
Withdrawal	August 6, 2024, 10:52 AM	11.21639738	\$700,000.00

Unchained Account			
Transaction Type	Date/Time	BTC	USD Value
Trade Executed	August 6, 2024, 8:00 PM	35.18614864	\$2,000,000.00
Deposit	August 7, 2024, 1:07 PM	35.18614864	\$2,000,000.00
Trade Settled	August 7, 2024, 3:07 PM	35.18614864	\$2,000,000.00
Withdrawal	August 7, 2024, 8:46 PM	35.18614864	\$2,000,000.00
Trade Executed	August 10, 2024, 4:06 PM	56.73051537	\$3,500,000.00
Deposit	August 13, 2024 8:14 AM	56.73051537	\$3,500,000.00
Withdrawal	August 13, 2024 9:55 AM	56.73051537	\$3,500,000.00
Trade Settled	August 13, 2024, 10:14 AM	56.73051537	\$3,500,000.00
Trade Executed	August 13, 2024, 7:18 PM	57.17605236	\$3,500,000.00
Deposit	August 15, 2024 7:42 AM	57.17605236	\$3,500,000.00
Trade Settled	August 15, 2024, 9:41 AM	57.17605236	\$3,500,000.00
Withdrawal	August 15, 2024 11:19 AM	57.17605236	\$3,500,000.00
Trade Executed	August 26, 2024, 11:40 AM	77.58390244	\$5,000,000.00
Deposit	August 27, 2024 1:01 PM	77.58390244	\$5,000,000.00
Trade Settled	August 27, 2024, 3:01 PM	77.58390244	\$5,000,000.00
Withdrawal	August 28, 2024 11:00 AM	77.58390244	\$5,000,000.00
Trade Executed	September 11, 2024, 7:06 PM	60.32141739	\$3,500,000.00
Deposit	September 12, 2024 12:42 AM	60.32141739	\$3,500,000.00
Withdrawal	September 12, 2024 12:42 AM	60.32141739	\$3,500,000.00
Trade Settled	September 12, 2024, 2:42 PM	60.32141739	\$3,500,000.00
TOTAL			\$18,500,000.00

201. As noted in the chart immediately above, UNCHAINED -- on several occasions -- permitted assets to be withdrawn from [REDACTED] account before the deposit had even been settled; which again speaks to anomalous business practices that run afoul of BSA and AML regulations.

//

//

FEDERAL REGULATIONS IMPOSE UPON DEFENDANTS REQUIREMENTS THAT THEY INVESTIGATE, REPORT, AND PREVENT SUSPICIOUS TRANSACTIONS AND ELDER FINANCIAL ABUSE

202. The Bank Secrecy Act (“BSA”) and its implementing regulations -- with which all Defendants must adhere -- impose an obligation on financial institutions to file a report of each deposit, withdrawal, exchange of currency or other payment or transfer, by, through, or to such financial institution which involves a transaction in currency of more than \$10,000, including multiple transactions that aggregate to more than \$10,000.⁵

203. A financial institution must file a Currency Transaction Report (CTR) within fifteen (15) days after the transaction is conducted.⁶

204. Accurate, complete, and timely CTRs are critical to the utility of BSA data in combating financial crimes and other illicit activity.

205. Additionally, a bank must identify suspicious transactions relevant to a possible violation of law or regulation in Suspicious Activity Reports (SARs) filed with the U.S. Department of the Treasury’s Financial Crimes Enforcement Network (“FinCEN”).⁷

206. Specifically, the BSA and its implementing regulations require banks to report transactions that involve or aggregate to at least \$5,000.00, are conducted or attempted by, at, or through the bank, and that the bank “knows, suspects, or has reason to suspect” are suspicious.⁸

207. A transaction is “suspicious” if a bank “knows, suspects, or has reason to suspect” that the transaction: (i) involves funds derived from illegal activities, or is conducted to disguise funds derived from illegal activities; (ii) is designed to evade the reporting or recordkeeping requirements of the BSA or regulations implementing it; or (iii) has no business or apparent lawful purpose or is not the sort in which the customer normally would be expected to engage, and the bank knows of no

⁵ 31 U.S.C. § 5313; 31 C.F.R. § 1010.311 (banks “shall file a report of each deposit, withdrawal, exchange of currency or other payment or transfer, by, though, or to such financial institution which involves a transaction in currency of more than \$10,000”); *see also* 31 C.F.R. §§ 1010.310, 1010.313(b).

⁶ 31 C.F.R. § 1020.310; 31 C.F.R. § 1010.306(a)(1).

⁷ 31 U.S.C. § 5318(g); 31 C.F.R. § 1020.320.

⁸ *Id.*

1 reasonable explanation for the transaction after examining the available facts, including background
2 and possible purpose of the transaction.⁹

3 208. Such suspicious activity includes elder abuse. In fact, in April 2013, the SAR forms
4 were amended to include a category of suspicious activity specifically for elder financial exploitation.

5 209. The reporting and transparency that financial institutions provide through these reports
6 is essential financial intelligence that FinCEN, law enforcement, and others use to safeguard the U.S.
7 financial system and combat serious threats, including money laundering, terrorist financing, organized
8 crime, corruption, drug trafficking, and massive fraud schemes targeting the U.S. government,
9 businesses, and individuals.¹⁰

10 210. To be able to identify suspicious activity and report it to FinCEN, banks have policies
11 and procedures to handle each type of transaction in which customers engage, including deposits,
12 checks, wire transfers, and cash transactions.

13 211. Banks utilize automated account monitoring systems that run in the background
14 reviewing all the transactions that are occurring at the bank. The automated account monitoring
15 systems will alert when transactions occur which contain red flags of money laundering or other
16 financial fraud. This includes patterns of elder abuse.

17 212. The bank's BSA analysts then review the transactions which alerted to determine if the
18 transactions are suspicious. If they are suspicious, the bank is required to file a SAR with FinCEN.

19 213. The standard in the banking industry is then to stop the suspicious transactions and close
20 accounts that have suspicious activity to prevent money laundering or other financial fraud from
21 continuing.

22 214. Wire transfers are at high risk for money laundering or other financial fraud. Banks'
23 automated account monitoring systems will alert if wire transfers contain red flags such as large, round
24 dollar amounts going in and out of an account on the same day or within a few days, or wire transfers
25 to and from high risk countries.

26 _____
27 ⁹ 31 C.F.R. § 1020.320(a)(2).

28 ¹⁰ FinCEN, FIN-2014-A007, FinCEN Advisory to U.S. Financial Institutions on Promoting a Culture of Compliance (Aug. 11, 2014).

1 215. These regulations, and others, have long been aimed at protecting not just financial
2 institutions themselves but also financial institution customers in vulnerable demographic groups such
3 as senior citizens.

4 216. In 2011, the Department of Justice issued an Advisory containing red flags of elder
5 abuse to include the following:

6 “Warning signs of financial exploitation:

- 7 • Sudden changes in bank accounts or banking practices, including an
8 unexplained withdrawal of large sums of money by a person accompanying
9 the older adult.
- 10 • Unexplained sudden transfer of assets to a family member or someone
11 outside the family.
- 12 • The provision of services that are not necessary.”

13 217. In 2011, FinCEN also issued an Advisory to financial institutions regarding elder abuse
14 and elder financial exploitation and how to identify them. The Advisory contained red flags of elder
15 financial exploitation so financial institutions could identify elder abuse and report it. The red flags
16 included the following:

17 “Erratic or unusual banking transactions, or changes in banking patterns:

- 18 • Frequent large withdrawals...
- 19 • Debit transactions that are inconsistent for the elder
- 20 • Uncharacteristic attempts to wire large sums of money.”

21 218. In 2013, the Board of Governors of the Federal Reserve System and Consumer Financial
22 Protection Bureau joined with six other federal agencies in issuing an “Interagency Guidance on
23 Privacy Laws and Reporting Financial Abuse of Older Adults” (“Interagency Guidance”) to financial
24 institutions such as Defendant BofA. The Interagency Guidance underscored what by then was a well-
25 known problem to Defendants and the rest of the banking community:

26 *Recent studies suggest that financial exploitation is the most common form of elder*
27 *abuse . . . Older adults can become targets of financial exploitation by family*
28 *members, caregivers, scam artists, financial advisers, home repair contractors,*
 fiduciaries (such as agents under power of attorney and guardians), and others.

1 *Older adults are attractive targets because they may have significant assets or equity*
 2 *in their homes. They may be especially vulnerable due to isolation, cognitive decline,*
 3 *physical disability, health problems, and/or the recent loss of a partner, family*
 4 *member, or friend. **Financial institutions can play a key role in preventing and***
 5 ***detecting elder financial exploitation. A financial institution’s familiarity with***
 6 ***older adults it encounters may enable it to spot irregular transactions, account***
 7 ***activity, or behavior. Prompt reporting of suspected financial exploitation to adult***
 8 ***protective services, law enforcement, and/or long term ombudsmen can trigger***
 9 ***appropriate intervention, prevention of financial losses, and other remedies.***¹¹
 10 *(emphasis added)*

7 219. The importance of the role of financial institutions in preventing and reporting financial
 8 elder abuse is emphasized in the Interagency Guidelines, including specifically clarifying that financial
 9 institutions may observe financial exploitation and may report such conduct without violating an older
 10 adult’s privacy.¹²

11 220. Further, the Interagency Guidelines specifically identify the well-known hallmarks of
 12 financial abuse of older adults, including, but not limited to: “*Erratic or unusual banking transactions,*
 13 *or changes in banking patterns, such as. . . Uncharacteristic attempts to wire large sums of money.*”¹³

14 221. A single such banking transaction by an elderly customer signifies financial abuse of an
 15 elder, as defined by California law, that is specifically identifiable and preventable by Financial
 16 Institutions like Defendants.

17 222. In 2022, FinCEN issued another Advisory to financial institutions entitled “Advisory on
 18 Elder Financial Exploitation” that included “financial red flags” of elder financial exploitation,
 19 including the following:

- 20 • “Dormant accounts with large balances begin to show constant withdrawals.
- 21 • An older customer suddenly begins discussing and buying CVC (convertible
 22 virtual currency).
- 23 • Uncharacteristic, sudden, abnormally frequent or significant withdrawals of
 24 cash or transfers of assets from an older customer’s account.

25
 26

 27 ¹¹ https://files.consumerfinance.gov/f/201309_cfpb_elder-abuse-guidance.pdf.

28 ¹² *Id.*

¹³ *Id.*

- Frequent large withdrawals.
- Debit transactions that are inconsistent for the older customer.
- Uncharacteristic attempts to wire large sums of money.”¹⁴

223. In the instant matter, many of those “financial red flags” were noticeably waving in front of Defendants, but they ignored or failed to pay heed to those warnings as they collected ever-increasing fees from Plaintiffs for the transactions flowing through their accounts.

DEFENDANTS HAD ACTUAL KNOWLEDGE, BUT FAILED TO HALT, THAT PLAINTIFFS WERE THE VICTIM OF ELDER FINANCIAL ABUSE

224. Within days of the first wire transfer on July 9, 2024, Plaintiffs’ investment and banking patterns -- each transaction of which Defendants actively facilitated -- so blatantly demonstrated elder financial abuse that Defendants had actual knowledge of, and substantially assisted in, the abuse for the subsequent weeks, to the point that Plaintiffs’ life savings were nearly depleted.

225. Further, BofA, for example, knew that all eight of the suspicious wire transfers made from Plaintiffs’ BofA account exceeded the U.S. Department of Treasury’s \$10,000.00 threshold requiring the filing of a “Currency Transaction Report,” thereby invoking the scrutiny of BofA’s management. That scrutiny would have necessarily focused upon (and thereby informed BofA’s management of) the identity of the customer initiating the suspicious wire transfers, the amount of the suspicious transactions, and the identity of the recipients.

226. Despite the fact that the very first wire transfer from one of Plaintiffs’ Charles Schwab accounts was for five-times the Department of Treasury’s threshold, and the first wire transfer from Plaintiffs’ BofA account was **thirty times** higher than that threshold, Charles Schwab and BofA employees continued to knowingly and substantially assist the blatant financial elder abuse, completing more than a dozen transfers of over a million dollars each.

227. In the meantime, Charles Schwab and BofA continued to charge Plaintiffs for each of the wire transfers that drained Plaintiffs’ accounts.

¹⁴ FinCEN Advisory on Elder Abuse, FIN-2022-A002 (June 15, 2022), available at <https://www.fincen.gov/sites/default/files/advisory/2022-06-15/FinCEN%20Advisory%20Elder%20Financial%20Exploitation%20FINAL%20508.pdf>.

1 228. Moreover, when Charles Schwab’s account monitoring software alerted it to lucrative
2 albeit anomalous activity in Plaintiffs’ accounts, Charles Schwab -- rather than inquire or halt that
3 clearly suspicious activity in Plaintiffs’ long-stable accounts -- sought to upsell Plaintiffs on additional
4 Charles Schwab services so Charles Schwab could cull larger fees from Plaintiffs.

5 229. When federal legislation such as the 2009 CARD Act clamped down on certain
6 predatory pricing practices by national banks (*e.g.*, high late fees, interest rate hikes, expensive
7 overdraft protection), many of those banks, including BofA, looked for new sources of revenue to make
8 up for what they lost. One new source was a higher fee for making wire transfers.¹⁵

9 230. Charles Schwab and BofA provide employee training on developing their abilities to
10 sell Charles Schwab and BofA products of services, and complete transactions correctly, but provide
11 grossly inadequate training of their representatives on their duty not to assist in elder financial abuse or
12 on how to report and prevent elder financial abuse.

13 231. Because Charles Schwab and BofA spend so much more time training their
14 representatives to sell products and services than they do training their representatives to spot and stop
15 financial elder abuse, those skewed priorities left their representatives far more prepared to earn the fee
16 they charge for asset transfers than to stop the blatantly unlawful elder financial abuse they were
17 substantially assisting in this case.

18 232. In fact, all Defendants knew or must have known that the activity constituted financial
19 elder abuse. Additionally, Charles Schwab and BofA had clear, actual knowledge that the activity
20 constituted financial elder abuse as described by Interagency Guidance, discussed above.

21 233. Financial elder abuse causes irreparable and devastating harm to its elderly victims, as
22 occurred here. By the time the financial elder abuse is discovered by the victims, the original
23 perpetrator has usually spent or otherwise siphoned off the elderly victims’ assets. Efforts at restitution,
24 therefore, are highly unlikely to yield any recovery of assets. The elderly victim often experiences a
25 permanent decline in his or her standard of living. Many victims suffer even more from feelings of
26 betrayal that typically accompany financial abuse.

27
28 ¹⁵ <https://www.newyorker.com/business/currency/the-high-cost-for-the-poor-of-using-a-bank>.

1 234. It was only when the FBI intervened and Plaintiffs received a return of the cash balance
2 that resided in ████████ UNCHAINED account on September 18, 2024 that any of the Defendants
3 took any affirmative actions to prevent further harm to Plaintiffs in the course of this orchestrated elder
4 abuse scam.

5 235. That step was far too late for Plaintiffs, though, who by that point had already suffered
6 losses of no less than \$18,500,000.00.

7 236. To be clear, each Defendant was not just warned about what was happening to Plaintiffs.
8 Each independently had actual knowledge based on the anomalous and suspicious behavioral activity
9 taking place in Plaintiffs' accounts that something was wrong, something criminal was happening; and
10 each Defendant had the independent ability to stop the victimization of Plaintiffs as each Defendant is
11 independently legal, ethically, and morally required to do -- an ability that remained unexercised until
12 it was too late for Plaintiffs.

13 237. Prior to filing this lawsuit, Plaintiffs and/or undersigned counsel communicated with
14 each of the Defendants to address the fraud perpetrated upon Plaintiffs and to demand that Defendants
15 provide restitution to Plaintiffs for the wrongful transactions each Defendant processed. Other than the
16 one wire transfer reversed by UNCHAINED, Defendants have failed or refused to provide Plaintiffs
17 any restitution or appropriate remedy for their harm.

18 238. Plaintiffs have duly performed all of their duties and obligations, and any conditions
19 precedent to Plaintiffs bringing this action have occurred, have been performed, or else have been
20 excused or waived.

21 239. To enforce their rights, Plaintiffs have retained undersigned counsel and are obligated
22 to pay counsel a reasonable fee for its services, for which Defendants are liable pursuant to Cal. Welf.
23 & Inst. Code § 15657.5, as a result of their bad faith, and otherwise.

24 //
25 //
26 //
27 //
28 //

CLAIMS FOR RELIEF

COUNT I

**Violation of the Elder Abuse and Dependent Adult Civil Protection Act
Cal. Welf. & Inst. Code § 15600, *et seq.*
(All Defendants)**

1
2
3
4 Plaintiffs reallege and incorporate by reference each and every allegation in paragraphs 1
5 through 239 inclusive, as if they were fully set forth herein.

6 240. This cause of action asserts against Defendants a claim for financial-elder abuse under
7 California Welfare & Institutions Code § 15610.30(a)(2), which imposes liability on a person or entity
8 that “assists” another in “tak[ing] . . . real or personal property of an elder.”

9 241. Specifically, Section 15610.30 provides the following, in pertinent part:

10 (a) “Financial abuse” of an elder or dependent adult occurs when a person or entity
11 does any of the following:

12 (1) Takes, secretes, appropriates, obtains, or retains real or personal property
13 of an elder or dependent adult for a wrongful use or with intent to defraud, or
14 both.

15 (2) Assists in taking, secreting, appropriating, obtaining, or retaining real or
16 personal property of an elder or dependent adult for a wrongful use or with
17 intent to defraud, or both. . . .

18 (b) A person or entity shall be deemed to have taken, secreted, appropriated,
19 obtained, or retained property for a wrongful use if, among other things, the
20 person or entity takes, secretes, appropriates, obtains, or retains the property and
21 the person or entity knew or should have known that this conduct is likely to be
22 harmful to the elder or dependent adult.

23 Cal. Welf. & Inst. Code § 15610.30(a)(1)–(2), (b) (emphasis added).

24 242. At all times relevant to this Complaint, Plaintiffs were residents of California and elders
25 within the meaning of the California Welfare & Institutions Code § 15600, *et seq.*

26 243. Defendants assisted in taking Plaintiffs’ property when they completed eight wire
27 transfers amounting to \$22,000,000.00 in furtherance of an elder financial abuse scheme.

28 244. Moreover, Defendants had actual knowledge that Plaintiffs were the victims of a fraud
perpetrated by the non-party recipient of Plaintiffs’ wire transfers.

245. Under California law, a defendant’s actual knowledge may be shown not only by direct
evidence but also by circumstantial evidence that the defendant must have known under the

1 circumstances of the facts alleged.

2 246. Here, Defendants knew that their conduct was likely to be harmful to Plaintiffs at least
3 because:

- 4 (a) Defendants knew Plaintiffs were elders, and that because of their age, Plaintiffs
5 were substantially more vulnerable to the deceptive taking of their savings and
6 assets.
- 7 (b) Plaintiffs are long-time TD Ameritrade/Charles Schwab customers, and their
8 investment advisor (Tony J. Kim) was aware that, prior to the events at issue in
9 this action, Plaintiffs had never liquidated or withdrawn assets held in their
10 accounts in any amount anywhere close in measure to the \$30,000,000.00 worth
11 of assets abruptly liquidated, and largely withdrawn, from Plaintiffs' accounts at
12 the behest of the Schwab Threat Actor. A portfolio liquidation and withdrawal
13 in that amount is highly anomalous and required a focused inquiry of the action
14 in Plaintiffs' accounts, of which there was none.
- 15 (c) Plaintiffs are long-time BofA customers, and BofA records reflect that, prior to
16 the events at issue in this action, Plaintiffs had not sent a wire transfer for several
17 years, if any such wire transactions were ever undertaken at BofA.
- 18 (d) Moreover, prior to the events at issue in this action, Plaintiffs only engaged in
19 limited banking activities and held in their BofA account a relatively modest
20 amount of funds; and the massive influx of tens of millions of dollars' worth of
21 funds that commenced in July 2024 were highly anomalous and required a
22 heightened level of scrutiny and inquiry that BofA did not provide. In fact, as
23 the Schwab Threat Actor increased the illicit flow of funds through Plaintiffs'
24 BofA account, BofA -- rather than increase its scrutiny of Plaintiffs' account
25 activity -- upgraded Plaintiffs from "Platinum Honors" status to "Diamond"
26 status as BofA discerned additional profit was available to it.
- 27 (e) BofA records reflect that after the bank branch Plaintiffs usually visited in their
28 home town of Walnut, California refused to process any wire transfers
subsequent to the initial transfer of \$300,000.00 under a suspicion of fraudulent
activity, the BofA branch in Diamond Bar, California readily authorized all
subsequent wire transfer requests without paying heed to any notation in BofA's
own records of suspected fraud and without heed to the frequency and amount of
funds being transferred.
- (f) the same BofA branch in Diamond Bar, California processed seven of Plaintiffs'
highly unusual, quick-succession wire transfers, such that it had actual
knowledge Plaintiffs were the victims of an elder-abuse scheme that was being
perpetuated via the wire transfers -- as a series of high-amount, quick-succession
transfers have the hallmark signs of financial elder abuse.
- (g) ████████ is a very short-time UNCHAINED customer; and despite the hallmarks
of financial improprieties (especially for an elderly customer), UNCHAINED

1 permitted in [REDACTED] UNCHAINED account a series of high-amount, quick-
2 succession deposits and withdrawals -- sometimes in the same day, which
3 amounts to highly suspicious activity at a cryptocurrency exchange but which
4 UNCHAINED permitted to go forward unchecked.

- 5 (h) Defendants are mandated reporters of suspected financial abuse of an elder adult
6 pursuant to Cal. Welf. & Inst. Code § 15630.1. Defendants were in direct contact
7 with Plaintiffs, reviewed their financial documents, records, and transactions in
8 connection with providing financial services to them, gave investment and
9 banking advice, and, within the scope of their professional practice, observed and
10 knew that Plaintiffs' sudden, suspicious, and highly unusual investment and
11 banking activity reasonably appeared to be financial abuse.
- 12 (i) Defendants observed and had knowledge of behavior and unusual circumstances
13 and transactions that would lead an individual with adequate training or
14 experience, based on the same facts, to form a reasonable belief that Plaintiffs
15 were the victims of financial abuse of elders.
- 16 (j) Defendants' own policies dictate for the continuous monitoring of such
17 suspicious activity.

18 247. Due to Charles Schwab's policies, knowledge and expertise, the failure to report,
19 prevent or delay the suspicious liquidation of valuable long-held assets and transfers of tens of millions
20 of dollars from Plaintiffs' Charles Schwab accounts over only a handful of weeks, and in some cases
21 within a matter of days, constituted assisting in the taking of funds from Plaintiffs for a wrongful
22 purpose, with the intent to defraud, and/or undue influence.

23 248. Likewise, due to BofA's policies, knowledge and expertise, the failure to report, prevent
24 or delay the suspicious transfers of tens of millions of dollars from Plaintiffs' BofA account over only
25 a handful of weeks, and in some cases within a matter of days, constituted assisting in the taking of
26 funds from Plaintiffs for a wrongful purpose, with the intent to defraud, and/or undue influence.

27 249. Similarly, due to UNCHAINED's policies, knowledge and expertise, the failure to
28 report, prevent or delay many of the suspicious transfers of tens of millions of dollars into and out of
[REDACTED] UNCHAINED account over only a handful of weeks, and in some cases within a matter of
days, constituted assisting in the taking of funds from Plaintiffs for a wrongful purpose, with the intent
to defraud, and/or undue influence.

29 250. As a direct and proximate result of Defendants' acts and omissions, Plaintiffs have
suffered damage.

1 251. Defendants' conduct was a substantial factor in cause Plaintiffs' harm.

2 252. The actions taken by Defendants set forth above were in all respects reckless, fraudulent,
3 oppressive, and/or malicious, and manifested conscious disregard for Plaintiffs' rights.

4 253. Plaintiffs are informed and believe, and on that basis allege, that these willful,
5 oppressive, fraudulent and/or malicious acts as alleged herein above were ratified by the officers,
6 directors, and/or managing agents of the Defendants.

7 254. Plaintiffs are therefore entitled to an award of exemplary and punitive damages pursuant
8 to California Civil Code § 3294, according to proof at trial.

9 255. Plaintiffs are entitled to compensatory damages, including general and special damages,
10 in an amount according to proof at time of trial.

11 256. Additionally, Plaintiffs are entitled to reasonable attorney's fees and costs pursuant to
12 Cal. Welf. & Inst. Code § 15657.5.

13 **COUNT II**
14 **Violation of California's Unfair Competition Law**
15 **Bus. & Prof Code § 17200**
16 **(All Defendants)**

17 Plaintiffs reallege and incorporate by reference each and every allegation in paragraphs 1
18 through 239 inclusive, as if they were fully set forth herein.

19 257. Defendants' conduct was unlawful, unfair, and/or fraudulent within the meaning of
20 Business & Professions Code § 17200.

21 258. Defendants' conduct was unlawful within the meaning of Business & Professions Code
22 § 17200 in that, among other conduct and statutes, Defendants' conduct violated Cal. Welf. & Inst.
23 Code § 15630.1 *et seq.*, as described in this Complaint.

24 259. Among other things, Defendants' agents and representatives failed to protect Plaintiffs,
25 who are elders within the meaning of the California Welfare & Institutions Code and residents of
26 California, from predatory elder financial abuse, by failing to follow their own fraud monitoring,
27 prevention and protection policies and transferring millions of dollars of Plaintiffs' funds via wire
28 transfers and failing to fulfill their reporting requirements pursuant to Cal. Welf. & Inst. Code §
15630.1.

1 260. Defendants' actions are part of a general business practice that was effectuated by
2 numerous agents and representatives across various different locations in this jurisdiction.

3 261. By reason of the acts and conduct alleged herein, Plaintiffs have suffered injury in fact.

4 262. Defendants have derived economic benefit by failing to follow their fraud prevention
5 and protection policies and assisting in the taking of Plaintiffs' funds from the accounts Plaintiffs
6 maintained with Defendants. Plaintiffs have a right to an order requiring Defendants to restore
7 Plaintiffs' money and interest, which may have been acquired by unfair, unlawful and/or fraudulent
8 business practices, as well as the resulting general damages.

9 263. Pursuant to Business & Professions Code § 17203, Plaintiffs seek from Defendants
10 restitution of all earnings, profits, compensation and benefit it obtained from Plaintiffs, as a result of
11 its conduct in violation of Business & Professions Code §§ 17200 *et seq.*, as described herein.

12 264. Plaintiffs further seek injunctive relief preventing Defendants from collecting on any
13 outstanding debts owed by Plaintiffs to Defendants.

14 **COUNT III**
15 **Gross Negligence**
16 **(All Defendants)**

17 Plaintiffs reallege and incorporate by reference each and every allegation in paragraphs 1
18 through 238 inclusive, as if they were fully set forth herein.

19 265. Defendants owed a duty to Plaintiffs to exercise reasonable care in safeguarding,
20 securing, and protecting Plaintiffs' accounts and assets from being compromised, lost, stolen and/or
21 misused in acts of apparent money laundering. This duty included, among other things, designing,
22 maintaining, and testing Defendants' automated security measures to ensure they were sufficient.

23 266. As financial institutions and licensed money transmitters, Defendants were obligated,
24 among other things, to comply with the BSA and its KYC/AML provisions.

25 267. Defendants had a duty to ensure that the security measures they advertised to customers
26 worked properly, including but not limited to, auto-detection of suspicious activity in customer
27 accounts that ran afoul of the BSA.

28 268. Defendants were all aware of Plaintiffs' advanced age.

1 269. By being entrusted by elder Plaintiffs to safeguard their accounts and assets, Defendants
2 had a special relationship with Plaintiffs.

3 270. Defendants knew they were the gatekeepers for Plaintiffs' accounts and valuable assets.

4 271. Defendants likewise knew that Plaintiffs' accounts and assets were vulnerable to
5 compromise and misuse by thieves and other criminals as they acknowledged in blog posts, industry
6 presentations, and other public statements.

7 272. Defendants thus knew of the substantial and foreseeable harm that could occur to
8 Plaintiffs if they did not implement proper KYC/AML and security measures to guard Plaintiffs'
9 accounts and assets and/or did not follow their own security measures.

10 273. Plaintiffs maintained accounts with Defendants and agreed to store valuable assets in
11 those accounts with the understanding that Defendants would take appropriate measures to protect
12 those accounts and assets.

13 274. Notwithstanding the trust they knew had been placed in them, Defendants did not protect
14 Plaintiffs' accounts and assets and violated their trust.

15 275. Defendants are morally culpable, given that they not only failed to protect Plaintiffs'
16 accounts and their assets during a period in which Defendants had actual knowledge that elder abuse
17 was afoot but also because Defendants sought to seize upon the rapid increase in the flow of assets
18 through Plaintiffs' accounts – no matter how suspicious and anomalous that assets flow was – by
19 rewarding Plaintiffs and seeking to entice them to increase the services they were receiving from
20 Defendants.

21 276. Defendant knowingly breached their duty to exercise reasonable care in safeguarding
22 and protecting Plaintiffs' accounts and assets by failing to adopt, implement, and maintain adequate
23 security measures.

24 277. Once discovery begins, Plaintiffs anticipate uncovering evidence showing that
25 Defendants made intentional decisions to upsell Plaintiffs on additional account services while
26 Defendants bypassed, deactivated, and/or failed to implement appropriate security measures that would
27 have prevented Plaintiffs' harm, including but not limited to refusing to process electronic and wire
28 transfers and permitting rapid deposits-and-withdrawals from Plaintiffs' accounts in a manner that

1 evidenced clear BSA violations.

2 278. But for Defendants’ known wrongful and negligent breach of their duties owed to
3 Plaintiffs, Plaintiffs’ assets would not have been stolen by an unauthorized person.

4 279. Defendants’ gross negligence was a direct and legal cause of Plaintiffs’ loss and the
5 legal cause of their resulting damages, including, but not limited to, the theft of their assets and massive
6 unwanted tax liabilities imposed upon Plaintiffs.

7 280. The injuries and harm suffered by Plaintiffs were the reasonably foreseeable result of
8 Defendants’ known failure to exercise reasonable care in safeguarding and protecting Plaintiffs’
9 accounts and their assets.

10 281. Defendants’ misconduct as alleged herein is malice, fraud, or oppression in that it was
11 despicable conduct carried on by Defendants, through Defendants’ officers; directors; and managing
12 agents, with a willful and conscious disregard of the rights or safety of Plaintiffs and despicable conduct
13 that has subjected Plaintiffs to cruel and unjust hardship in conscious disregard of their rights.

14 282. Absent authorization and/or ratification by Defendants’ officers, directors, and
15 managing agents to forgo adequate security measures and to fail to halt transactions that were obvious
16 signs of elder abuse and of BSA violations, the harm to Plaintiffs could not have occurred. As a result,
17 Plaintiffs are entitled to punitive damages against Defendants.

18 **COUNT IV**
19 **Violations of Section 1693g of the Electronic Funds Transfer Act and Section 1005.6(B) of**
20 **Federal Regulation E with respect to**
21 **Unauthorized Transfers from ██████████ Account**
22 **(against Defendant UNCHAINED)**

23 Plaintiffs reallege and incorporate by reference each and every allegation in paragraphs 1
24 through 239 inclusive, as if they were fully set forth herein.

25 **A. Legal Framework of the EFTA**

26 283. The Electronic Funds Transfer Act (“EFTA”) and its corresponding regulations
27 implemented by the Consumer Financial Protection Bureau (“CFPB”), 12 C.F.R. § 1005.1, *et seq.* were
28 designed with the “primary objective” of “the provision of individual consumer rights.” 15 U.S.C. §
1693; 12 C.F.R. § 1005.1(b) (the “primary objective of the act and this part is the protection of
individual consumers engaging in electronic fund transfers and remittance transfers.”). The primary

1 purpose of the EFTA and Federal Regulation E is to protect individual consumers engaging in
2 electronic fund transfers and remittance transfers.

3 284. The following definitions under the EFTA and Federal Regulation E, among others, are
4 particularly relevant to the instant dispute:

- 5 (a) A “financial institution” means “a bank, savings association, credit union, or any
6 other person that directly or indirectly holds an account belonging to a consumer,
7 or that issues an access device and agrees with a consumer to provide electronic
8 fund transfer services”;
- 9 (b) The term “account” means “a demand deposit (checking), savings, or other
10 consumer asset account (other than an occasional or incidental credit balance in
11 a credit plan) held directly or indirectly by a financial institution and established
12 primarily for personal, family, or household purposes.”
- 13 (c) The term “consumer” means a “natural person”;
- 14 (d) The term “Access device” means a “card, code, or other means of access to a
15 consumer's account, or any combination thereof, that may be used by the
16 consumer to initiate electronic fund transfers.”
- 17 (e) An access device becomes an “accepted access device” when the consumer: (i)
18 requests and receives, or signs, or uses (or authorizes another to use) the access
19 device to transfer money between accounts or to obtain money, property, or
20 services; (ii) requests validation of an access device issued on an unsolicited
21 basis; or (iii) receives an access device in renewal of, or in substitution for, an
22 accepted access device from either the financial institution that initially issued
23 the device or a successor.
- 24 (f) The term “electronic fund transfer” means any “transfer of funds that is initiated
25 through an electronic terminal, telephone, computer, or magnetic tape for the
26 purpose of ordering, instructing, or authorizing a financial institution to debit or
27 credit a consumer’s account”;
- 28 (g) The term “Unauthorized electronic fund transfer” means an “electronic fund
transfer from a consumer’s account initiated by a person other than the consumer
without actual authority to initiate the transfer and from which the consumer
receives no benefit.” The term does not include, as relevant here, “a person who
was furnished the access device to the consumer’s account by the consumer.”

24 **B. Factual Allegations**

25 285. UNCHAINED is a “financial institution,” as defined by the EFTA and Federal
26 Regulation E, because it is a company that directly or indirectly holds accounts belonging to consumers,
27 including ██████ account, and because UNCHAINED issues an access device and agrees with a
28 consumer to provide electronic fund transfer services. 15 U.S.C. § 1693a(9); 12 C.F.R. § 1005.2(i).

1 286. ██████ is a “consumer,” as defined by the EFTA and Federal Regulation E, because he
2 is a natural person. 15 U.S.C. § 1693(a)(6); 12 C.F.R. § 1005.2(j).

3 287. ██████ UNCHAINED account is an “account,” as defined by the EFTA and Federal
4 Regulation E, because it is a consumer asset account held directly or indirectly by UNCHAINED and
5 established primarily for personal, family, or household purposes. 15 U.S.C. § 1693a(2); 12 C.F.R.
6 1005.2(b)(1). ██████ account was used for such personal purposes – *i.e.*, intended to earn income
7 from appreciating assets – and not for business purposes.

8 288. ██████ UNCHAINED account is an “access device,” as defined by Federal
9 Regulation E, because it is used by a consumer to initiate electronic fund transfers to or from a consumer
10 account. ██████ UNCHAINED account holds a private key that allows a consumer to initiate
11 electronic fund transfers.

12 289. The electronic funds that were transferred from ██████ UNCHAINED account are
13 “unauthorized electronic fund transfers” because they were initiated by a person other than the owner
14 of the account by fraud and without consent, and without actual authority to initiate such transfer, from
15 which ██████ received no benefit. The primary purpose of the electronic transfers was for the Schwab
16 Threat Actor to steal ██████ cryptocurrency assets and not for investment in a liquidity pool. Further,
17 as directly applicable here, an “unauthorized EFT includes a transfer initiated by a person who obtained
18 the access device from the consumer through fraud or robbery.” *See*, 12 CFR 1005.2 Comment 2(m).
19 That is what happened here.

20 290. Pursuant to the EFTA, the liability of a consumer, such as ██████ for unauthorized
21 electronic funds transfers is limited to the lesser of \$50.00, or the amount of money or value of property
22 or services obtained in such unauthorized electronic fund transfer prior to the time that the financial
23 institution is notified of, or otherwise becomes aware of, circumstances which lead to the reasonable
24 belief that an unauthorized electronic fund transfer involving the consumer’s account has or may be
25 effected.

26 291. As alleged above, UNCHAINED received notice from ██████ that there were
27 unauthorized electronic transfers from ██████ UNCHAINED account. Section 1693g(a)(2) of the
28 EFTA provides that: “Notice under this paragraph is sufficient when such steps have been taken as may

1 be reasonably required in the ordinary course of business to provide the financial institution with the
2 pertinent information, whether or not any particular officer, employee, or agent of the financial
3 institution does in fact receive such information.” Similarly, Section 1005.6(b)(5) provides that:
4 “Notice to a financial institution is given when a consumer takes steps reasonably necessary to provide
5 the institution with the pertinent information, whether or not a particular employee or agent of the
6 institution actually receives the information.”

7 292. After receiving notice from [REDACTED] [REDACTED] of the unauthorized electronic transfers,
8 UNCHAINED failed to refund [REDACTED] UNCHAINED account for the unauthorized transfers as
9 required by the EFTA and Federal Regulation E.

10 293. In addition, UNCHAINED failed to timely investigate the unauthorized electronic
11 transfers from [REDACTED] UNCHAINED account as required by 15 U.S. Code § 1693f(a)(3) and 15 U.S.
12 Code § 1693f(d) by failing to conduct a reasonable review of its own records. See, 12 C.F.R. §
13 205.11(c)(4); see also, Supp. I to § 205 at 11(c) 4–5. Indeed, an adequate investigation would have
14 easily led UNCHAINED to the conclusion that fraud had occurred given that [REDACTED] did not authorize
15 the transfers at issue, that there were security flaws on UNCHAINED’s platform, and that fraudulent
16 transfers had been widely reported as a common issue to UNCHAINED.

17 294. UNCHAINED’s limitation of liability provision in its User Agreement is inapplicable
18 because pursuant to § 1693l of the EFTA: “No writing or other agreement between a consumer and any
19 other person may contain any provision which constitutes a waiver of any right conferred or cause of
20 action created by this subchapter.”

21 295. Based on the foregoing, and pursuant to the EFTA and Federal Regulation E,
22 UNCHAINED is required to refund [REDACTED] for all of his losses due to unauthorized electronic transfers
23 from his UNCHAINED account at current valuations, including interest thereon, an additional amount
24 not less than \$100, and the costs of the action, together with reasonable attorneys’ fees.

25 296. In the alternative, if UNCHAINED is not deemed to either directly or indirectly hold
26 [REDACTED] account, UNCHAINED is still liable, pursuant to 12 C.F.R. § 1005.14, for the unauthorized
27 electronic transfers; because UNCHAINED provided the electronic fund transfer service to [REDACTED]
28 from other financial institutions without an agreement with the account-holding institution.

COUNT V

**Violations of Section 1693c of the Electronic Funds Transfer Act and
Section 1005.6 of Federal Regulation E with respect to
Failure to Make Required Disclosures
(against Defendant UNCHAINED)**

1 Plaintiffs reallege and incorporate by reference each and every allegation in paragraphs 1
2 through 239 inclusive, as if they were fully set forth herein.

3
4 297. Pursuant to § 1693c of the EFTA, UNCHAINED is required to disclose, amongst other
5 things, at the time the consumer contracts for an electronic fund transfer service: (i) the consumer's
6 liability for unauthorized electronic fund transfers; (ii) the telephone number and address of the person
7 or office to be notified in the event the consumer believes that an unauthorized electronic fund transfer
8 has been or may be effected; (iii) a summary, in a form prescribed by regulations of the Bureau, of the
9 error resolution provisions of section 1693f and the consumer's rights thereunder; and (iv) under what
10 circumstances the financial institution will in the ordinary course of business disclose information
11 concerning the consumer's account to third persons.

12
13 298. Similarly, pursuant to § 1005.7 of Federal Regulation E, UNCHAINED is required to
14 disclose, among other things: (i) a summary of the consumer's liability for unauthorized electronic fund
15 transfers; (ii) the telephone number and address of the person or office to be notified when the consumer
16 believes that an unauthorized electronic fund transfer has been or may be made; and (iii) notice of the
17 error resolution provision.

18
19 299. UNCHAINED failed to make the proper disclosures as required by the EFTA and
20 Federal Regulation E.

21 300. UNCHAINED's Terms of Service and Privacy Policy did not disclose the consumer's
22 liability for unauthorized electronic fund transfers as required by the EFTA and Federal Regulation E.
23 Instead, UNCHAINED included a limitation of liability provision which purported to discharge
24 UNCHAINED from any liability under any circumstances for damages arising out of or in any way
25 related to software, products, services, and/or information offered or provided by third parties and
26 accessed through the app, site or services.

27 301. UNCHAINED did not include a telephone number and address for the person or office
28 [REDACTED] should notify if he believed an unauthorized electronic fund transfer occurred, as required by

1 the EFTA and Regulation E.

2 302. UNCHAINED failed to disclose the error resolution provision, as required by the EFTA
3 and Federal Regulation E.

4 303. UNCHAINED failed to disclose that it would share [REDACTED] private key with third
5 parties to establish the fraudulent smart contracts and failed to have proper security mechanisms in
6 place under an AI sequencing protocol.

7 304. Based on the foregoing, and pursuant to the EFTA and Federal Regulation E,
8 UNCHAINED is required to refund [REDACTED] for his losses at current valuations due to the unauthorized
9 electronic transfers from his UNCHAINED account, including interest thereon, an additional amount
10 not less than \$100, and the costs of the action, together with reasonable attorney's fees.

11 **COUNT VI**

12 **Violations of Section 1693f of the Electronic Funds Transfer Act and**
13 **Section 1005.11 of Federal Regulation E With Respect to**
14 **Failure to Utilize Proper Procedures for Resolving Errors**
(against Defendant UNCHAINED)

15 Plaintiffs reallege and incorporate by reference each and every allegation in paragraphs 1
16 through 239 inclusive, as if they were fully set forth herein.

17 305. The procedures for resolving errors of Federal Regulation E and the EFTA provides, in
18 relevant part, that if a financial institution receives notice of an error within sixty days after having sent
19 the periodic statement or transmitted to a consumer documentation of an electronic funds transfer,
20 receives oral or written notice in which the consumer: (i) enables the institution to identify the
21 consumer's name and account number; (ii) indicates why the consumer believes an error exists; and
22 (iii) includes to the extent possible the type, date, and amount of the error, the financial institution must
23 promptly investigate the alleged error, determine whether an error has occurred, and report or mail the
24 results of such investigation and determination to the consumer within ten business days. 15 U.S.C. §
25 1693f(a)(3); 12 C.F.R. § 1005.11(b)(1).

26 306. If the financial institution determines that an error did occur, it has the option to either:
27 (1) timely correct the error, including the crediting of interest where applicable; or (2) timely
28 provisionally recredit the consumer's account for the amount alleged to be in error pending the

1 conclusion of the institution's investigation of the error within ten business days of being notified of
2 the error. 15 U.S.C. § 1693(f)(c); see also, 12 C.F.R. § 1005.11.

3 307. In no circumstance can an investigation be concluded more than forty-five (45) days
4 after receipt of the notice of error, and during the pendency of the investigation, the consumer must be
5 allowed full use of funds provisionally recredited. *Id.*

6 308. Since UNCHAINED failed to disclose the error resolution procedures, [REDACTED]
7 pursuant to 15 U.S.C. § 1693g and/or 12 C.F.R. § 1005.6, is not liable for any amount of the
8 unauthorized transfers.

9 309. Moreover, UNCHAINED failed to timely investigate the unauthorized transfers from
10 [REDACTED] account as required by 15 U.S.C. § 1693f(a)(3) and 15 U.S.C. § 1693d by failing to conduct
11 a timely and reasonable review of its own records. Indeed, an adequate investigation would have easily
12 revealed that [REDACTED] was the victim of identity theft and an account takeover permitted by
13 UNCHAINED.

14 310. If UNCHAINED actually conducted a reasonable investigation, it would have
15 concluded that [REDACTED] did not authorize the transfers at issue, the fraudulent transfers were made to
16 accounts other than those owned, controlled, or authorized by [REDACTED] and that fraudulent transfers
17 like the ones to which [REDACTED] was a victim had been widely reported as common problems on the
18 UNCHAINED platform.

19 311. Since UNCHAINED failed to provisionally recredit [REDACTED] account within the ten-
20 day period and did not make a good faith investigation of the unauthorized transfer, pursuant to §
21 1693f(e)(1), [REDACTED] is entitled to treble damages.

22 312. Moreover, pursuant to 1693f(e)(2), [REDACTED] is entitled to treble damages because
23 UNCHAINED knowingly and willfully concluded that [REDACTED] account was not in error when no
24 other reasonable conclusion could have been drawn from the evidence available to UNCHAINED at
25 the time it should have been investigating [REDACTED] claims.

26 //

27 //

28 //

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs [REDACTED] an individual, and [REDACTED] an individual; respectfully pray for relief against Defendants THE CHARLES SCHWAB CORPORATION, a Delaware corporation; CHARLES SCHWAB BANK, SSB, a Texas-chartered state savings bank; BANK OF AMERICA, N.A., a national banking association; and UNCHAINED TRADING, LLC, a Texas limited liability company; as follows:

- (a) A judgment awarding Plaintiffs equitable restitution including, without limitation, restoration of the *status quo ante* and return to Plaintiffs all cryptocurrency or fiat currency -- as well as a trade correction reversing all unauthorized sell trades and returning to Plaintiffs all shares of stock -- illicitly taken from them in connection with the fraudulent and abusive scheme allowed and perpetrated by Defendants;
- (b) Entry of injunctive relief to prevent Defendants from collecting from Plaintiffs any outstanding debts;
- (c) An award of any and all additional damages recoverable under law including but not limited to compensatory damages, special damages, punitive damages, incidental damages, and consequential damages;
- (d) Pre- and post-judgment interest;
- (e) Attorneys' fees, expenses, and the costs of this action; and
- (f) All other and further relief as the Court deems necessary, just, and proper.

DEMAND FOR JURY TRIAL

Pursuant to Rule 38 of the Federal Rules of Civil Procedure, Plaintiffs demand trial by jury in this action of all issues so triable.

RESERVATION OF RIGHTS

Plaintiffs reserve their right to further amend this Complaint, upon completion of their investigation and discovery, to assert any additional claims for relief against Defendants or other parties as may be warranted under the circumstances and as allowed by law.

DATED: October 23, 2024

Respectfully submitted,

By: /s/ Karl S. Kronenberger
Karl S. Kronenberger, Esq.
CA Bar No. 226112
KRONENBERGER ROSENFELD, LLP

548 Market Street, #85399
San Francisco, CA 94104
Telephone: (415) 955-1155
E-Mail: Karl@kr.law

David C. Silver, Esq. (*pro hac vice* forthcoming)
Eric F. Rosenberg, Esq. (*pro hac vice*
forthcoming)

SILVER MILLER
4450 NW 126th Avenue - Suite 101
Coral Springs, Florida 33065
Telephone: (954) 516-6000
E-Mail: DSilver@SilverMillerLaw.com
E-Mail: ERosenberg@SilverMillerLaw.com

Attorneys for Plaintiffs [REDACTED]
and [REDACTED]

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28