IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

MICHAEL B. ZIDELL, MICHAEL B. ZIDELL 1997 EXEMPT LIFETIME TRUST, and MICHAEL B. ZIDELL 2016 EXEMPT LIFETIME TRUST,	§	
Plaintiffs,	§	**Civil Action No. _____**
vs.	§	
	§	**JURY TRIAL DEMANDED**
CITIBANK, N.A.,	§	
Defendant.	§	

PLAINTIFFS' ORIGINAL COMPLAINT

Plaintiff Michael B. Zidell, ("Plaintiff Zidell"), the Michael B. Zidell 1997 Exempt Lifetime Trust ("Plaintiff 1997 Trust"), and the Michael B. Zidell 2016 Exempt Lifetime Trust ("Plaintiff 2016 Trust") files Plaintiffs' Original Complaint against Defendant Citibank, N.A. ("Citibank" or "Defendant") and respectfully states as follows:

I.

PRELIMINARY STATEMENT

Romance scam. Rug pull. Pig butchering.[1] These are just some of the terms to describe the scam that befell the Plaintiffs.

[1] According to the Financial Industry Regulatory Authority, "pig butchering" is so "named in reference to the practice of fattening a pig before slaughter, these scams often involve fraudsters contacting targets seemingly at random, then gaining trust before ultimately manipulating their targets into phony investments and disappearing with the funds. ¶ Pig butchering schemes often start with solicitations of modest investments intended to bolster your confidence. They usually involve some type of fake claim or falsified dashboard that shows assets exponentially growing, with the intent being to encourage larger and larger investments." FINRA, "*'Pig Butchering' Scams: What They Are and How to Avoid Them,*" FINRA, December 13, 2022, https://www.finra.org/investors/insights/pig-butchering-scams.

Plaintiff Zidell was solicited on social media about an exciting investment opportunity — making a market for Non Fungible Tokens. It was an expensive scam.

Each species of scam is slightly different in nature and methodology, but in order to work, they all have something in common: a bank that turns a blind eye to its statutory duties and obligations, including Know-Your-Customer ("KYC") and Anti-Money Laundering ("AML") requirements. The bank — who was happy to take fees along the way to Plaintiffs' $20 million dollar ruin — have already been subjected to at least one government seizure arising from this scam. This lawsuit seeks relief from their failures.

II.

PARTIES

1. Plaintiff Michael B. Zidell is a individual and residing in Dallas County, Texas. He is a citizen of Texas.

2. Plaintiff Michael B. Zidell 1997 Exempt Lifetime Trust is a Texas trust. Michael B. Zidell serves as the Trustee for the 1997 Trust. Its Trustee is a citizen of Texas.

3. Plaintiff Michael B. Zidell 2016 Exempt Lifetime Trust is a Texas trust. Michael B. Zidell serves as the trustee for the 2016 Trust. Its Trustee is a citizen of Texas.

4. Defendant Citibank, N.A. is a national association with its headquarters located at 5800 South Corporate Place, Sioux Falls, South Dakota 57108. Its main office is located at 399 Park Avenue New York, NY 10022. Citibank, N.A. It may be served with process through CT Corporation System 28 Liberty St., New York, NY 10005.

5. Plaintiffs are informed and believe, and on that basis allege, that at all relevant times mentioned in this Complaint, Defendant was acting in concert and actively participating with those parties through whose accounts Plaintiffs' funds were deposited as set forth more fully below.

III.

JURISDICTION AND VENUE

10. This court has jurisdiction 28 U.S.C. § 1332 because all parties are the parties are citizens of different States and the amount in controversy exceeds $75,000.00, exclusive of interest and costs.

11. Venue is proper in this Court under 28 U.S.C. § 1391 (b)(2) because a substantial part of the events giving rise to the claims occurred in this District.

IV.

FACTUAL BACKGROUND

A. OpenrarityPro.com – "Investing" in the NFT market.

13. In January 2023, Plaintiff Zidell was contacted on Facebook by someone who said they were named Carolyn Parker ("Parker"). Parker represented that she was a business owner and lived in California. Parker and Plaintiff Zidell communicated by telephone and video chat on the WeChat app.

14. At first, Plaintiff Zidell felt that his communication with Parker was developing into a friendly, social relationship, but later perceived a romantic one developing. In February 2023, Parker told Plaintiff Zidell that she had invested in non-fungible tokens ("NFTs") and had earned millions of dollars in investment gains. Parker told Plaintiff Zidell that she invested on a website called "OpenrarityPro.com," (the "NFT Enterprise") and suggested that he invest there as well.

15. To be clear, "Openrarity.com" is one of largest NFT trading website in the world; it is not the same thing as the NFT Enterprise – OpenrarityPro.com.

16. Parker explained to Plaintiff Zidell that in investing as she described, he would be bidding on NFTs from various artists, and in exchange he would receive a daily investment return of up to 5% on his money.

17. As the "investment" was explained to Plaintiff Zidell, he would be helping to make a market for NFTs. His only obligations would be to provide funding and select from an array of NFTs while they were being bid upon. During one video chat, Parker showed Plaintiff Zidell an account statement purporting to show that she had earned millions of dollars with this investment activity in NFTs.

18. Starting in January 2023, Plaintiffs decided to invest in the NFT Enterprise as Parker suggested, and began to wire transfer funds to different bank accounts that were provided to him through the OpenrarityPro.com website. When Plaintiff Zidell asked a representative of OpenrarityPro.com why he was sending funds to different bank accounts, he was told that due to a large volume of customer deposits, multiple banks were needed to process all the customer investments. At the time, Plaintiff Zidell felt this was a reasonable explanation, and, over the next months, Plaintiffs sent forty-three wire transfers totaling over $20 million to different bank accounts.

19. All of Plaintiffs' investments and investment decisions were made in Texas based on representations received in Texas.

20. Plaintiffs' transfers to Defendant Citibank are as follows:

Transaction Date	Amount	Victim	Recipient Bank	Name on Recipient Account	Routing Number (last four)	Account Number (last four)
2/15/2023	$442,000	1997 Trust	Citibank	Guju, Inc.	0089	1187
2/15/2023	$400,000	1997 Trust	Citibank	Guju, Inc.	0089	1187

2/15/2023	$341,000	2016 Trust	Citibank	Guju, Inc.	0089	1187
2/15/2023	$300,000	2016 Trust	Citibank	Guju, Inc.	0089	1187
2/21/2023	$431,000	1997 Trust	Citibank	Guju, Inc.	0089	1187
2/21/2023	$467,000	2016 Trust	Citibank	Guju, Inc.	0089	1187
2/23/2023	$324,000	2016 Trust	Citibank	Guju, Inc.	0089	1187
2/23/2023	$433,000	1997 Trust	Citibank	Guju, Inc.	0089	1187
2/27/2023	$423,000	2016 Trust	Citibank	Guju, Inc.	0089	1187
2/27/2023	$198,000	1997 Trust	Citibank	Guju, Inc.	0089	1187
3/1/2023	$112,400	2016 Trust	Citibank	Guju, Inc.	0089	1187
3/1/2023	$72,500	1997 Trust	Citibank	Guju, Inc.	0089	1187
Total:	**$3,943,900**					

21. In March 2023, Plaintiff Zidell checked his account balance on the OpenrarityPro.com website, which purported to show that his balance was now over $300 million. Plaintiff Zidell requested to withdraw some of his funds from OpenrarityPro.com but was told that to obtain his funds he would have to send funds to cover a "risk deposit." Plaintiff Zidell agreed to pay and did send those funds. After sending the additional funds, Plaintiff Zidell requested funds from his account, but was once again told he had to pay additional fees to have his funds withdrawn.

22. By late-April, the OpenrarityPro.com website was all of a sudden gone. It was a classic "rug pull," or "exit scam" in which developers make promises, then quickly "exit" with investors' funds. Literally, there was nowhere for Plaintiffs to turn. At this time, Plaintiff Zidell suspected he was a victim of fraud, felt embarrassed he fell for a scam, and reported his case to the Dallas Police Department and the FBI.

B. The Banks and their Regulatory Environment – what *should* happen.

23. Defendant Citibank is primarily regulated by the Office of the Comptroller of the Currency. Its RSSD ID is 476810.

24. Defendant is subject to, *inter alia*, the Bank Secrecy Act, 31 U.S.C. § 5311, *et seq.* ("BSA"). Specially, Defendant is a financial institution as defined by 31 U.S.C. § 5312(a)(2).

25. Federal law requires banks to "know their customers." *See, e.g.*, 31 C.F.R. § 1020.220. As Federally regulated banks, Defendant must adhere to KYC obligations, conducting customer due diligence to gauge the risk of fraud, money laundering, terrorist financing, or other illicit account uses.

26. Among other things, Defendant is required to understand the types of transactions in which their customers are likely to engage and to remain vigilant for transactions that may be suspicious. These laws impose upon Defendant a duty to understand the nature and purpose of their customer relationships and to develop a customer risk profile. This information must then be used for ongoing monitoring of its customers' transactions. Such duties form part of the federally mandated compliance with Anti-Money-Laundering ("AML") laws. *See, e.g.*, 31 C.F.R. § 1020.210.

27. Defendant is also required by law to establish and maintain procedures reasonably designed to assure and monitor their compliance with the requirements of the BSA. *See* 12 C.F.R. § 21.21.

28. When monitoring its customers' accounts, Defendant is obligated to comply with the BSA, including regulations broadening its AML provisions. The BSA requires Defendant to develop, administer and maintain a program to ensure compliance. That program must be approved by each bank's board of directors and noted in the board meeting minutes, and must (1) provide

for a system of internal controls to ensure ongoing BSA compliance, (2) provide for independent testing of the bank's compliance, (3) designate an individual to coordinate and monitor compliance and (4) provide training for appropriate personnel.

29. Defendant must also maintain a customer due diligence program to predict the types of transactions, dollar volume and transaction volume each customer is likely to conduct, thereby providing the bank with a means of identifying unusual or suspicious transactions for each customer. The customer due diligence program allows the bank to maintain awareness of the financial activity of its customers and the ability to predict the type and frequency of transactions in which its customers are likely to engage.

30. The Federal Financial Institutions Examination Council ("FFIEC") sets standards and guidelines for banks to comply with their AML obligations. FFIEC publications describe certain "red flags" that indicate possible money laundering schemes and other misconduct requiring further inquiry. Defendant must be able to identify and take appropriate action once put on notice of any of a series of money laundering indicia set forth in the Federal Financial Institutions Examination Council's BSA/AML Examination Manual.

31. The FFIEC BSA/AML Examination manual identifies a host of "red flags" to alert Defendant as to suspicious activity. Many are present in this matter:

a. Funds Transfers

i. "Many funds transfers are sent in large, round dollar, hundred dollar, or thousand dollar amounts.

ii. Funds transfer activity occurs to or from a financial secrecy haven, or to or from a higher-risk geographic location without an apparent business reason or when the activity is inconsistent with the customer's business or history.

iii. Funds transfer activity occurs to or from a financial institution located in a higher risk jurisdiction distant from the customer's operations.

iv. Many small, incoming transfers of funds are received, or deposits are made using checks and money orders. Almost immediately, all or most of the transfers or deposits are wired to another city or country in a manner inconsistent with the customer's business or history.

v. Funds transfer activity is unexplained, repetitive, or shows unusual patterns.

vi. Payments or receipts with no apparent links to legitimate contracts, goods, or services are received.

vii. Funds transfers are sent or received from the same person to or from different accounts.

viii. Funds transfers contain limited content and lack related party information."

b. Other Unusual or Suspicious Activity

i. "Customer receives large and frequent deposits from online payments systems yet has no apparent online or auction business.

ii. Unusual use of trust funds in business transactions or other financial activity.

iii. Customer conducts large deposits and withdrawals during a short time period after opening and then subsequently closes the account or the account becomes dormant. Conversely, an account with little activity may suddenly experience large deposit and withdrawal activity.

iv. Customer makes high-value transactions not commensurate with the customer's known incomes."

The source for these red flags is the FFIEC BSA/AML Appendices - Appendix F – "Money Laundering and Terrorist Financing Red Flags."

C. What *didn't* happen.

32. In applying these rules and standards, Defendant's due diligence programs should have been built to tailor scrutiny towards their high-risk customers. Defendant should have placed into effect customer identification and due diligence programs in a manner that allows them to (i) know who is in charge of each account, (ii) the nature and purpose of the account and the customer's business, and (iii) the anticipated transactions that will be processed through the account, together with expected volume and frequency.

33. That clearly did not happen here.

34. In the account opening documents for Defendant Citibank's accounts for Guju, Inc., their customer states that it will receive no wire transfers, and the total value of the wires it would out would be less than $250,000 per month. In fact, the wires they say they will send are $8,000 transfers to China. The reality was obviously different. The account received no less than twelve (12) wires from Plaintiffs and dozens from others. Some of the outbound wires exceeded $2,000,000.00. Even worse, the account stated an annual gross revenue of $300,000 and Guju received more than 12 times that amount from Plaintiffs alone in two weeks. The first wire from Plaintiffs exceeded Guju's stated annual revenue by almost 50%.

35. Defendant's obligations were clear; as shown herein, they wholly failed to discharge them.

D. *United States v. $811,549.41, et al.* – A Verified Complaint for Forfeiture

36. In October of 2023, the United States filed Case No. 2:23-cv-08774 in the U.S. District Court for the Central District of California a verified complaint for forfeiture against various funds held by the Defendant (and another, unrelated bank).

37. In that matter, the United States claimed that the "defendant bank funds constitute or are derived from proceeds traceable to violations of 18 U.S.C. § 1343 (wire fraud), which is a specified unlawful activity as defined in 18 U.S.C. §§ 1956(c)(7)(A) and 1961(1). The defendant bank funds are therefore subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(C)."

38. The United States further claimed that the "defendant bank funds constitute property involved in multiple transactions or attempted transactions in violation of 18 U.S.C. § 1956(a)(1)(A)(i) or (a)(1)(B)(i), or property traceable to such property, with the specified unlawful activity being violations of 18 U.S.C. § 1343. The defendant bank funds are therefore subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(A)."

39. Defendant did not contest the forfeiture.

40. In order to be entitled to relief, the United States had to, and in fact did, prove wire fraud had occurred.

41. As a result, the United States seized and returned to Plaintiff Zidell "$1,260,874.44 of the Defendant Funds."

42. A welcome recovery, but with this suit, Plaintiffs seek to obtain more than that symbolic amount of justice.

V.

CAUSES OF ACTION

A. COUNT ONE: AIDING AND ABETTING (NY)

43. Plaintiffs incorporate and reallege all previous allegations as if fully set forth herein.

44. As detailed above, Carolyn Parker and her unknown accomplices (including through their entities who were transferees from the Defendant) offered and/or sold securities to Plaintiffs by means of untrue statements or omissions of material facts necessary to make the statements made, in light of the circumstances under which they were made, not misleading, all in violation of New York law.

45. The NFT Enterprise was not licensed to sell securities.

46. Plaintiffs invested money into an investment contract, the NFT Enterprise.

47. Plaintiffs were to receive daily interest on their monies supporting the NFT Enterprise.

48. Plaintiffs expected to receive profits from their investments in the NFT Enterprise.

49. The profits from the NFT Enterprise investment were to be derived primarily from the efforts of the managers of the NFT Enterprise.

50. Defendant is liable as an aider and abettor as it, directly or indirectly, knew of the tortious conduct of the NFT Enterprise because the transactions at issue expressly contradicted the account opening documents and violated AML/KYC "red flags." Defendant materially aided the seller or issuer of a security and are, therefore, jointly and severally liable with the seller or issuer and to the same extent as the seller or issuer.

51. As detailed above, Defendant through its recklessness, provided substantial assistance to Parker and her co-conspirators by opening bank accounts, providing services including wire transfers and allowing them to be used to perpetrate the NFT Enterprise scam in violation of their explicit KYC and AML obligations.

52. Plaintiffs seek compensatory damages.

B. COUNT TWO: AIDING AND ABETTING SECURITIES FRAUD (TX)

53. Plaintiffs incorporate and reallege all previous allegations as if fully set forth herein.

54. As detailed above, Carolyn Parker and her unknown accomplices (including through their entities who were transferees from the Defendant) offered and/or sold securities to Plaintiffs by means of untrue statements or omissions of material facts necessary to make the statements made, in light of the circumstances under which they were made, not misleading, in violation of TEX. GOV. CODE § 4008.052.

55. The NFT Enterprise was not licensed to sell securities.

56. Plaintiffs invested money into an investment contract, the NFT Enterprise.

57. Plaintiffs were to receive daily interest on their monies supporting the NFT Enterprise.

58. Plaintiffs expected to receive profits from their investments in the NFT Enterprise.

59. The profits from the NFT Enterprise investment were to be derived primarily from the efforts of the managers of the NFT Enterprise.

60. Pursuant to TEX. GOV. CODE § 4008.055(c), Defendant is liable as aiders and abettors as it, directly or indirectly, acted with reckless disregard for the truth or the law materially and materially aided the seller or issuer of a security and are, therefore, jointly and severally liable with the seller or issuer and to the same extent as the seller, buyer, or issuer.

61. As detailed above, Defendant through its recklessness, materially aided Parker and her co-conspirators by opening bank accounts, providing services including wire transfers and allowing them to be used to perpetrate the NFT Enterprise scam in violation of their explicit KYC and AML obligations.

62. Plaintiffs seek compensatory damages as allowed by TEX. GOV. CODE § 4008.057.

63. Plaintiffs seek their costs and attorneys' fees as allowed by TEX. GOV. CODE § 4008.060.

C. COUNT THREE: NEGLIGENCE (NY)

64. Defendant had a duty to exercise due care in monitoring suspicious transactions.

65. Defendant's duty to Plaintiffs falls into the "narrowly circumscribed" duty to third parties (1) not to ignore red flags or suspicious circumstances that may indicate that a third party involved in that transaction is being defrauded, and, in that instance, (2) not to proceed with the transaction without first doing some investigation to dispel those suspicions. As stated above, the large, round numbers of funds along, among other things, should have triggered the bank's investigation into the suspicious activity.

66. Defendant failed to implement adequate securities measures, failed to detect clearly suspicious transactions and failed to monitor the accounts even though large, round sums were transferred in and out of the accounts from trusts and other individuals in a suspicious manner, and, last, Defendant failed to provide timely warnings about known scams.

67. Defendant's failure to exercise due care resulted in Plaintiffs losing large amount of funds as a result of the scam.

68. Plaintiffs were significantly damaged as a result of Defendant's failures.

VI.

JURY DEMAND

65. Plaintiffs respectfully demand trial by jury.

VII.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray for Judgment as follows:

a. A judgment in Plaintiffs' favor and against Defendant on all of Plaintiffs' claims against Defendant;

b. For compensatory damages;

c. That the Court award Plaintiffs their attorneys' fees, costs, and expert fees, as allowed by law;

d. An award of prejudgment and post judgment interest, as provided by law; and

e. Such other and further relief to which Plaintiffs may be justly entitled.

Respectfully submitted,

/s/ Aaron R. Easley
Aaron R. Easley (ae9922)

SESSIONS ISRAEL & SHARTLE, LLC
3 Cross Creek Drive
Flemington, NJ 08822-4938
(504) 828-3700 (Main)
(908) 237-1660 (Direct)
(732) 423-1177 (Facsimile)
aeasley@sessions.legal

ATTORNEYS FOR PLAINTIFFS