THE AMERICAN ARBITRATION ASSOCIATION

----------X

In the Matter of the Arbitration Between:

[redacted]

Claimant,

DEMAND FOR ARBITRATION

- against -

[redacted]

Respondents.

----------X

[redacted] ("Claimant"), by their undersigned attorneys, files herein this Demand for Arbitration against [redacted] (collectively, "Respondent" "Respondents" or "Coinbase") and in support thereof states to the Arbitrator as follows:

JURISDICTION, CONSUMER RULES, ARBITRATOR AND HEARING LOCATION

1. The Claimant was, at all material times, a user of Coinbase.

2. Respondent and Claimant are parties to an arbitration agreement (the, "User Agreement"), which mandates that any disputes be adjudicated through the American Arbitration Association under its Consumer Rules with California law governing.

3. Claimant objects to the fairness of the parties' contact, but wishes to proceed in arbitration.

4. Claimant requests a three-day virtual hearing to be conducted over Zoom.

PARTIES AND RELEVANT NON-PARTY

[redacted]

7. [redacted]

[redacted]

FACTS

9. Coinbase is one of the largest cryptocurrency exchange platforms in the world, purportedly serving over 100 million verified users across more than 100 countries.

10. Coinbase holds billions of dollars in customer assets, including both cryptocurrencies and fiat currencies such as U.S. dollars and euros.

11. According to publicly disclosed financials, Coinbase routinely manages ***more than $100 billion in assets on its platform***, and processes billions in transaction volume monthly.

12. Coinbase is heavily regulated at both the federal and state levels.

13. Federally, Coinbase is licensed with the "Financial Crimes Enforcement Network," or FinCEN, which is a bureau within the Department of Treasury. Coinbase is licensed as a "money service business," or MSB, through FinCEN.

14. As a licensed MSB, Coinbase must (i) maintain an effective, written anti-money-laundering program reasonably designed to prevent money laundering and other unlawful activity, pursuant to 31 C.F.R. § 1022.210; and (ii) monitor for and report all suspicious activity by filing Suspicious Activity Reports (SARs) as required by 31 U.S.C. § 5318(g) and 31 C.F.R. § 1022.320.

15. Coinbase must also engage in transaction and account-based monitoring as an MSB. see FIN-2019-G001 ("Subject: Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies").

16. Separately, as a non-bank "financial institution" under Title V of the Gramm-Leach-Bliley Act (GLBA), Coinbase must protect customers' nonpublic personal information by implementing an information security program, which encrypts and protects customer data.

17. Coinbase has similar obligations at the state level.

18. At the state level, Coinbase holds a "BitLicense" issued by the New York State Department of Financial Services (NYDFS) under 23 NYCRR Part 200. Coinbase holds similar regulatory licenses in numerous other states, which it publicly discloses on its website.

19. These individual state licenses each impose strict cybersecurity, capital, and custodial requirements.

20. As a regulated heavily entity, Coinbase must protect customer funds using rigorous cybersecurity systems aligned with industry best practices. These systems are designed to prevent account takeovers, theft and other illegal activity.

21. [redacted]

[redacted]

28. Coinbase openly admits to events like these occurring. For example, in May 2025, Coinbase posted the following on its website:

> Cyber criminals bribed and recruited a group of rogue overseas support agents to steal Coinbase customer data to facilitate social engineering attacks. These insiders abused their access to customer support systems to steal the account data for a small subset of customers. No passwords, private keys, or funds were exposed and Coinbase Prime accounts are untouched. We will reimburse customers who were tricked into sending funds to the attacker. We're cooperating closely with law enforcement to pursue the harshest penalties possible and will not pay the $20 million ransom demand we received. Instead we are establishing a $20 million reward fund for information leading to the arrest and conviction of the criminals responsible for this attack.[1]

[1] Available here: https://www.coinbase.com/es-es/blog/protecting-our-customers-standing-up-to-extortionists

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

CLAIMANT'S CAUSES OF ACTION

COUNT I
(VIOLATION OF EFTA)

32. Claimant restates, and incorporates herein by reference, every paragraph contained in this Demand for Arbitration.

33. Claimant is an individual and not a professional currency trader.

34. Claimant views cryptocurrencies as a replacement for real currencies and not as a speculative asset like stocks or bonds.

35. Claimant did not purchase cryptocurrency as an "investment."

36. Rather, Claimant purchased all their cryptocurrency because they are distrustful of traditional banks and the United States Dollar. Claimant utilizes cryptocurrency as a proxy for a traditional bank account.

37. The primary purpose of the Electronic Funds Transfer Act, or "EFTA" and Federal Regulation E is the protection of individual consumers engaging in electronic fund transfers and remittance transfers.

38. Coinbase is a "financial institution" as defined by the EFTA and Federal Regulation E because it is a company that directly or indirectly holds accounts belonging to consumers,

including Claimant's account. see *Rider v. Uphold HQ Inc*., 657 F.Supp 3d 491 (S.D.N.Y. Feb. 22, 2023) (crypto exchanges are subject to EFTA).

39. Claimant is a "consumer" as defined by the EFTA and Federal Regulation E because they are a natural person. 15 U.S.C. § 1693(a)(6); 12 C.F.R. § 1005.2(j).

40. Claimant's accounts are "accounts" as defined by the EFTA and Federal Regulation E because they are consumer asset accounts held directly or indirectly by Coinbase and established primarily for personal, family, or household purposes. 15 U.S.C. § 1693a(2); 12 C.F.R. § 1005.2(b)(1). see *Nero v. Uphold HQ Inc*., 2023 U.S. Dist. LEXIS 149562 (SDNY Aug. 23 2023).

41. The electronic funds that were transferred from Claimant's account were "unauthorized electronic fund transfers" because they were initiated by a person other than the owner of the account by fraud and without consent, and without actual authority to initiate such transfer, from which Claimants received no benefit.

42. Significantly, an "unauthorized EFT includes a transfer initiated by a person who obtained the access device from the consumer through fraud or robbery." See 12 CFR 1005.2 Comment 2(m).

43. Critically, financial institutions are liable for unauthorized electronic transfers ***even if the customer's conduct is negligent***. ("Electronic Funds Transfers FAQ," published by the Consumer Financial Protection Bureau and last updated December 13, 2021, Page 13, Question 7).

44. In, *Garcia v. Navy Fed. Credit Union*, 2025 U.S. Dist. LEXIS 70829 (SD Cal. April 14, 2025) the Court explained the trier of fact should not consider the customer's negligence if a third party secured access to the account through fraud. Here is the Court's reasoning:

> Plaintiff argues that the means of access to his account were obtained through fraud, and he therefore never truly "furnished" the fraudulent user with his information, pointing to interpreting regulations by the Federal Reserve Board and Consumer Financial Protection Bureau ("CFPB"). Doc. No. 81 at 27. ***Both support interpretations that "[a]n***

> ***unauthorized [transfer] includes a transfer initiated by a person who obtained the access device from the consumer through fraud or robbery."*** 12 C.F.R. § 205, Supp. I at 2(m)(3) (Fed. Reserve Bd.); 12 C.F.R. § 1005, Supp. I at 2(m)(3) (CFPB) (same). Plaintiff also points to a case from the Southern District of New York, citing both regulations and holding that account information furnished under fraudulent pretenses is not "authorized" under the EFTA. *Green v. Cap. One*, N.A., 557 F. Supp. 3d 441, 447-48 (S.D.N.Y. 2021).
>
> Having reviewed the law and considered the parties' arguments, the Court agrees with Plaintiff's reading. First, the idea that one can, through fraudulent inducement, "furnish" account information sufficient to fall under Section 1693a(12)(A) runs contrary to the rest of that provision, which exempts transfers initiated by one who has furnished said information, but the "consumer has [since] notified the financial institution involved that transfers by such other person are no longer authorized." 15 U.S.C. § 1693a(12)(A). This provision presumes a consumer's knowledge that the "authorized" user was intended or empowered to make transactions and, as the Green court notes, "it would be illogical to require a consumer to revoke the account access of an individual who was never intended to have such access in the first place, or else risk liability for any resulting unintended transfers." Green, 557 F. Supp. 3d at 448.
>
> (emphasis added).

45. Accordingly, financial institutions like Coinbase are liable for customer losses under EFTA even if the customer's actions were negligent under state law. This is because the sole purpose of EFTA is to shift the risk of loss associated with unauthorized electronic fund transfers from consumers to financial institutions.

46. As alleged above, Coinbase received notice from Claimant that there were unauthorized electronic transfers from Claimant's account.

47. After receiving notice from Claimant of the unauthorized electronic transfers, Coinbase failed to refund Claimant's account for the unauthorized transfers as required by the EFTA and Federal Regulation E.

48. Accordingly, Coinbase is liable to the Claimant for damages under EFTA, including treble damages, attorneys' fees and costs. See 15 USC § 1693.

COUNT II
(VIOLATION OF UCC 4A)

49. Claimant repeats and incorporates all preceding allegations as though fully set forth herein.

50. To the extent EFTA does not govern the unauthorized transfers at issue—this cause of action is asserted in the alternative under Article 4A of the California Uniform Commercial Code (Cal. Com. Code §§ 11201 et seq.).

51. Article 4A also governs the rights and responsibilities of parties involved in electronic funds transfer, including the issuance and execution of payment orders and wire transfers between financial institutions and their customers.

52. Under California Commercial Code § 11202 and related provisions, a receiving bank may accept a payment order issued in the name of a customer only if it employs a security procedure that is commercially reasonable and effectively verifies the identity of the person initiating the payment order.

53. Coinbase failed to implement or properly apply commercially reasonable security procedures in connection with the unauthorized transfers from Claimant's account.

54. As a result of these failures, Coinbase executed one or more unauthorized payment orders or withdrawals that were not validly authorized by Claimant.

55. These transactions do not constitute "authorized" transfers under California UCC Article 4A, and liability for the resulting losses rests with Coinbase, which failed to meet its statutory obligations of due care and verification.

56. Claimant sustained actual and consequential damages as a direct and proximate result of these unauthorized funds transfers, including but not limited to the loss of fiat funds, the loss of cryptocurrency assets purchased with those funds, and other financial injuries.

COUNT III
(CAL. BUS. & PROF. CODE § 17200)

57. Claimant incorporates by reference all preceding paragraphs of this Demand for Arbitration.

58. Under the California Unfair Competition Law ("UCL"), unfair competition is broadly defined to include any unlawful, unfair, or fraudulent business act or practice. See *Cel-Tech Commc'ns, Inc. v. L.A. Cellular Tel. Co*., 20 Cal. 4th 163, 180 (1999).

59. Coinbase falsely represents on its website that its platform is secure and that it employs robust account monitoring to protect its customers. These representations appear prominently on Coinbase.com, which is incorporated by reference.

60. Specifically, Coinbase states the following on its website:

> Our proprietary blockchain analytics software, called Coinbase Tracer, allows us to investigate illicit activities, screen risky transactions, monitor risk, trace the flow of funds, and analyze blockchain data. It's fully integrated into our transaction monitoring system, which is a proprietary tool with sophisticated scenarios covering both crypto and fiat activity.
>
> Using Tracer, we can screen crypto transactions in real time. If we identify an inbound transaction from a sanctioned address, we can automatically interdict it and transfer funds to an internal holding account where they are held securely. This process prevents sanctions violations from even happening – something we believe is novel in the industry.
>
> As is the case in traditional financial institutions, we use a Customer Risk Scoring system to assign customers a risk rating when they join Coinbase. This allows us to identify high-risk characteristics, including ones that are indicative of potentially unusual or indicative of bad intent. When we identify high-risk indicators, our team conducts a thorough assessment to determine whether we can onboard the customer and what mitigants we might need to apply.
>
> Unlike many other companies, however, our risk scoring system is dynamic — meaning we don't just score our customers when they join, or at a specific moment in time. Our system monitors for real time changes. This allows us to look for red flags in standard "know your

> customer" information, ***but also through location changes, asset flows, transactions, and other key information that is updated on a daily basis***.[2]
>
> (emphasis added)

61. These statements are false. Coinbase's platform is not secure and was vulnerable to the unauthorized access and theft described herein. Its monitoring systems failed to detect or prevent the fraudulent activity targeting Claimant's account.

62. Claimant reasonably relied on Coinbase's public representations to their detriment, including by entrusting digital assets to a platform that failed to meet the basic standards of care it advertised.

63. These misrepresentations constitute fraudulent and unlawful business practices under the UCL.

64. Claimant therefore demands full restitution of all cryptocurrency assets purchased or held on Coinbase's platform.

COUNT IV
(VIOLATION OF THE CALIFORNIA CONSUMER PRIVACY ACT)

65. Claimant restates and incorporates herein by reference every allegation contained in this Demand for Arbitration.

66. This dispute arose only because Respondent failed to protect consumer information. Respondent collected and maintained sensitive personal information about Claimant and other consumers and had a duty to safeguard that data. Respondent's inadequate security controls allowed unauthorized actors to obtain access to Claimant's account credentials and/or personal information.

[2] Available here: https://www.coinbase.com/blog/how-coinbase-identifies-bad-actors-and-keeps-the-ecosystem-safe

But for Respondent's failure to protect consumer information with reasonable security procedures and practices, the unauthorized access and resulting losses would not have occurred.

67. Respondent failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information it collected and maintained about Claimant. As a result of that failure, Claimant's nonencrypted and nonredacted personal information and/or Claimant's email address in combination with a password or security question and answer permitting access to the account were subject to unauthorized access and exfiltration, theft, or disclosure, thereby triggering the private right of action under Cal. Civ. Code § 1798.150.

68. The categories of personal information implicated include, without limitation, Claimant's name in combination with one or more data elements listed in Cal. Civ. Code § 1798.81.5(d)(1)(A) (including a financial account number with any required access code or other government-issued identifiers) and/or Claimant's email address together with a password or security question and answer that would permit access to Claimant's account.

69. As a direct and proximate result of Respondent's wrongful conduct and its failure to implement or enforce adequate protective measures, Claimant suffered substantial economic harm, including the loss of digital assets; time and out-of-pocket costs responding to and mitigating the incident; diminution of the value of Claimant's personal information; and the continued risk of identity theft and fraud.

70. To the extent required by Cal. Civ. Code § 1798.150(b), Claimant provided Respondent with written notice identifying the specific provisions alleged to have been violated and an opportunity to cure. Claimant alleges that implementation or maintenance of reasonable security procedures and practices following a breach does not constitute a "cure" with respect to that breach.

71. Claimant seeks statutory damages in an amount not less than $100 and not greater than $750 per consumer per incident, or actual damages, whichever is greater; injunctive and

declaratory relief (including an order requiring Respondent to implement and maintain reasonable security procedures and practices compliant with Cal. Civ. Code § 1798.81.5); and any other relief the Arbitrator deems proper.

COUNT V
(DECLARATORY RELIEF)

72. Claimant restates, and incorporates herein by reference, every paragraph contained in this Demand for Arbitration.

73. Coinbase requires its customers to subscribe to a contract of adhesion in order to use its services.

74. A contract of adhesion is defined as "a standardized contract, imposed upon the subscribing party without an opportunity to negotiate the terms." *Flores v. Transamerica HomeFirst, Inc.*, 93 Cal. App. 4th 846, 113 Cal. Rptr. 2d 376, 381-82 (Cal. Ct. App. 2001)

75. The contract between the Claimant and Coinbase is more than a garden variety contract of adhesion – it is procedurally and substantively unconscionable.

76. Here, Coinbase updates its terms of service multiple times per month. Respondent makes these updates with no notice whatsoever to customers, including the Claimant.

77. Coinbase does not even send customers an email notification when it unilaterally amends its terms of service. This makes the terms of service less like a contract and more like meaningless words that exist on the internet.

78. Unilaterally modifying an agreement without providing notice to the other party, renders an agreement procedurally unconscionable. see *Heckman v. Live Nation Ent., Inc*., 120 F.4th 670, 683 (9th Cir. 2024) quoting (*Peleg v. Neiman Marcus Grp., Inc*., 204 Cal. App. 4th 1425, 140 Cal. Rptr. 3d 38, 42 (Cal. Ct. App. 2012)).

79. In addition to being procedurally unconscionable, Respondent's terms are also substantively unconscionable.

80. "Substantive unconscionability pertains to the fairness of an agreement's actual terms and to assessments of whether they are overly harsh or one-sided." Heckman at 683 (internal citations omitted).

81. Coinbase's terms are substantively unconscionable because the terms contain numerous unfair provisions.

82. For example, Coinbase's terms of service purport to limit the Claimant's ability to seek discovery.

83. Most significantly, Respondent's terms contain a blanket, and unintelligible, waiver of liability in favor of Coinbase.

84. Respondent modified and expanded this liability waiver multiple times without providing notice to Claimant or its other customers.

85. There is an actual and justiciable controversy between Claimant and Respondent regarding the validity of Respondent's terms of service, including any purported liability waivers or restrictions contained therein.

86. Claimant hereby requests an order finding that Respondent's liability waiver is void as unconscionable.

COUNT VI
(BREACH OF THIRD PARTY CONTRACT)

87. Claimant restates, and incorporates herein by reference, every paragraph contained in this Demand for Arbitration.

88. Coinbase, at all relevant times, maintained "crime insurance" to protect against losses from theft.

89. According to its website:

> Coinbase is insured against theft and hacking in an amount that exceeds the average value of bitcoin we hold in online storage at any given time. The insurance covers losses due to breaches in physical or cyber security, accidental loss, and employee theft. It doesn't cover bitcoin lost or stolen as a result of an individual user's negligence to maintain secure control over their login credentials.

90. Coinbase has an agreement with various insurance companies to provide this insurance coverage to its customers.

91. Claimant is a third-party beneficiary of those agreements.

92. Coinbase's advertisement of this crime insurance on its website created a duty to its customers to submit a covered loss to the insurance carrier.

93. Coinbase materially breached its obligation to provide insurance coverage to the Claimant.

94. As a direct and proximate result of Coinbase's failures, Claimant suffered significant financial damages and is therefore, entitled to damages in an amount to be proven at arbitration, but in no case, less than the amount of cryptocurrencies lost to the hackers and the fees charged by Coinbase.

COUNT VII
(BREACH OF CONTRACT)

95. Claimant restates, and incorporates herein by reference, every paragraph contained in this Demand for Arbitration.

96. Coinbase, at all relevant times, agreed to act as a "custodian" of Claimant's funds.

97. According to the parties' contract:

> In order to more securely and effectively custody assets**,** Coinbase may use shared blockchain addresses, controlled by Coinbase, to hold Supported Digital Assets for Digital Asset Wallets on behalf of customers and/or held on behalf of Coinbase. Although we maintain

> separate ledgers for users' Coinbase Accounts and Coinbase accounts held by Coinbase for its own benefit, Coinbase shall have no obligation to create a segregated blockchain address for your Supported Digital Assets.

98. This foregoing means cryptocurrency is co-mingled with other customers' funds at Coinbase for enhanced security protection.

99. Under the parties' contract, Coinbase agrees to secure assets in this manner as an additional security feature.

100. Coinbase breached the parties' contract by failing to "securely and effectively" custody the Claimant's assets as described above.

101. As a direct and proximate result of Coinbase's failures, Claimant suffered significant financial damages and is therefore, entitled to damages in an amount to be proven at arbitration, but in no case, less than the amount of cryptocurrencies lost to the hackers and the fees charged by Coinbase.

COUNT VIII
(GROSS NEGLIGENCE)

102. Claimant restates and incorporates herein by reference every paragraph contained in this Demand for Arbitration.

103. Respondent, Coinbase, breached three distinct duties owed to Claimant, each of which independently supports a claim for negligence: (i) The duty to reasonably safeguard Claimant's personal confidential information; (ii) The duty to prudently monitor Claimant's account activity for signs of compromise; and (iii) The duty to monitor transactions for suspicious or unauthorized activity.

104. These duties are not discretionary.

105. They arise from multiple, overlapping legal and regulatory obligations.

106. First, as a virtual currency platform providing services to U.S. customers, Coinbase is subject to the Gramm-Leach-Bliley Act (GLBA), which requires financial institutions to implement and maintain reasonable policies and procedures to protect the security and confidentiality of customer information.

107. GLBA mandates a written information security program, risk assessments, and safeguards tailored to identified risks.

108. Second, Coinbase is further subject to industry-specific cybersecurity norms, including those outlined by applicable FinCEN guidance, which require robust systems to detect and respond to potentially suspicious or fraudulent activity.

109. Third, Coinbase has promulgated its own internal fraud prevention policies, security protocols, and monitoring procedures. These internal controls are not voluntary; they are a fundamental component of Coinbase's compliance with its regulatory obligations and public representations.

110. Fourth, Coinbase's obligations also stem from well-established norms in the cybersecurity industry, including the standards published by the National Institute of Standards and Technology (NIST), which set the baseline for reasonable care when safeguarding customer data and monitoring digital financial activity.

111. Fifth, Coinbase is also subject to state-level cyber security requirements in the states where it does business. For example, in New York, Coinbase is subject to 23 NYCRR § 500, which mandates written cybersecurity policies, risk assessments, and incident response procedures. Other states where Coinbase is licensed have similar requirements.

112. The facts of this case reveal a breakdown in each of the described protective systems.

113. The attacker should not have known Claimant's identity, contact information, or even that they held a Coinbase account. The root cause of this fraud was Coinbase's failure to safeguard Claimant's information, not any misconduct by Claimant.

114. If Coinbase had a system in place to protect Claimant's personal, confidential information, then that system failed.

115. Coinbase purportedly maintains real-time account-based monitoring systems designed to detect unauthorized access or account takeovers. These systems also failed.

116. The unauthorized access to Claimant's account should have triggered multiple internal alerts, including login attempts from new devices or locations, IP mismatches, behavioral anomalies, and transaction velocity indicators. Coinbase failed to act meaningfully in response to those red flags and others, which can only be learned through discovery since Coinbase is the sole party with access to this information.

117. Claimant will present expert testimony showing that Coinbase's account security controls fell below the standard of care expected of institutions entrusted with customer funds. These were not one-off errors, but systemic failures in Coinbase's detection and incident response capabilities.

118. Coinbase also failed to meet its obligations in transaction monitoring. Like other regulated financial platforms, Coinbase uses tools to screen outgoing transactions for potential links to fraud or illicit finance. These screening systems are not optional; they are required by law and by Coinbase's own representations to customers and regulators.

119. Coinbase has publicly touted its proprietary risk engine and dynamic transaction monitoring features.

120. It has claimed to employ adaptive models that account for geography, asset flows, behavioral shifts, and user-specific risk scores. Those systems simply failed to operate as promised.

121. Had Coinbase acted with reasonable diligence—consistent with its regulatory obligations, its own policies, and prevailing industry standards—Claimant's losses would have been prevented.

122. Coinbase's negligence, including its failure to safeguard customer information, monitor account activity, and respond to clear indicators of fraud, was the direct and proximate cause of Claimant's harm.

COUNT IX
(ELDER ABUSE)

123. Claimant restates, and incorporates herein by reference, every paragraph contained in this Statement of Claim.

124. Claimant is a senior citizen, as defined by California Welfare and Institutions Code section 15610.27.

125. The terms of service state that California law applies.

126. As such, Claimant falls under the protection of Welfare and Institutions Code section 15600, the Elder Abuse and Dependent Adult Civil Protection Act.

127. Under this Act, Respondents have committed "financial abuse," which is defined as:

> [W]hen a person or entity does any of the following: (1) Takes, secretes, appropriates, or retains real or personal property of an elder or dependent adult to a wrongful use or with intent to defraud, or both…

128. The Act also requires a finding of liability if Coinbase knows or should know that a third party was committing elder abuse.

129. This Act mandates that a prevailing claimant be awarded attorney's fees and costs:

> Where it is proven by clear and convincing evidence that a [respondent] is liable for ... financial abuse as defined in Section 15610.30, and that the [respondent] has been guilty of recklessness, oppression, fraud, or malice in the commission of this abuse, in addition to all other remedies provided by law: (a) The court shall award to the [claimant] reasonable attorney's fees and costs. The term "costs" includes, but is not limited to, reasonable fees for the services of a conservator, if any, devoted to the litigation of a claim brought under this article…

130. The law states that if victims of elder abuse are eligible to be awarded punitive damages, those damages may be trebled, if the person committing the acts at the elder's expense caused the elder to lose "substantial loss of property set aside for retirement, or for personal or family care and maintenance..." Civil Code § 3345.

131. As stated above, Claimant lost a significant portion of their nest egg, losses which would be considered substantial.

132. As a direct and proximate consequence of Respondent's wrongful conduct, Claimant suffered damages.

DAMAGES

Claimant hereby requests the following relief against the Respondent:

a. Compensatory damages in an amount no less than [redacted] USD or the actual cryptocurrency stolen from the Claimant, plus interest thereon;

b. Tripple damages in an amount of no less than [redacted] or three (3) times the actual cryptocurrency stolen from the Claimant pursuant to 15 USC § 1693.

c. Reasonable costs and attorneys' fees pursuant to 15 USC § 1693.

d. Restitution in the form of cryptocurrency or USD.

e. Punitive damages.

f. Such other relief the Arbitrator deems just and proper.

Dated: New York, New York
December 2, 2025

Respectfully submitted,

MDF LAW PLLC

By: *Marc Fitapelli, Esq.*
Jeffrey Saxon, Esq.
28 Liberty Street, 30th Floor
New York, New York 10005
Phone: (212) 203-9300
Fax: (855) 348-2735

Attorneys for Claimant