AMERICAN ARBITRATION ASSOCIATION® | INTERNATIONAL CENTRE FOR DISPUTE RESOLUTION®

AMERICAN ARBITRATION ASSOCIATION
Consumer Arbitration Rules

In the Matter of the Arbitration between

Case Number: 01-24-0003-1829

Ashok Maini
-vs-
Coinbase, Inc.

AWARD OF ARBITRATOR

I, Steven Michael Ruffalo, the undersigned arbitrator, having been designated in accordance with the arbitration agreement entered into between the above-named parties, and having been duly sworn, and having duly heard the proofs and allegations of the Parties, Claimant by counsel and Respondent by counsel, at the evidentiary hearings held on October 14, 2025, October 15, 2025, and October 16, 2025, do hereby issue this FINAL AWARD as follows:

PROCEDURAL BACKGROUND

An evidentiary hearing was conducted over 3 days, as noted above, and an official transcript was prepared and certified by Anne Vosburgh, CSR, RPR, CRR. The parties submitted both pre-hearing and post-hearing briefs and were permitted during the hearing to call the witnesses they chose to examine under oath in support of their respective positions. The parties further submitted individually and jointly a total of 309 exhibits for consideration in the hearing and moved their chosen exhibits into evidence jointly without objection on October 20, 2025, and all such exhibits have been admitted into evidence. Respondent further filed its Confidentiality Designations to which Claimant submitted Objections and a Motion to Strike following which Respondent filed its own Response. On November 3, 2025, I issued my Order that I would take the Designation and Objections under advisement to be ruled upon in this, my final decision. In the process of rendering my award pursuant to applicable Consumer Arbitration Rules (R-43 and R-44), I have read the entire record, all expert witness reports, all briefs submitted, and all exhibits submitted and moved into evidence.

Following my August 1, 2025, ruling on the Respondent's Motion for Summary Judgment, which was granted in part and denied in part, the claims which survived summary dismissal are, as submitted by Claimant for evidentiary hearing during this arbitration:

- Gross negligence
- Breach of contract and implied covenant of good faith
- Violation of California False Advertising Law
- Violation of the Electronic Funds Transfer Act (15 U.S.C. § 1693 et seq.)
- Fraudulent and negligent misrepresentation
- Violation of Cal. UCC § 8507(b) (ineffective entitlement orders)
- Breach of fiduciary duty

The defenses asserted by Respondent to these claims include:

- User Agreement disclaims liability for phishing or compromised credentials (Ex. J1 §§ 5.3, 6.6)

- Coinbase's security exceeds industry standards; no evidence competitors provide stronger protection (Tr.789:14-790:22)
- Claimant's own negligence—sharing credentials, ignoring warnings—broke the security chain (Tr.704:17-23) B. Contractual Claims (pp. 16)
- No breach of User Agreement or Privacy Policy; no material misrepresentations (Tr. 597:4-12) C. Statutory Claims (pp. 17–18)
- EFTA inapplicable: account "established primarily" for investment (15 U.S.C. § 1693a(2); *Yuille v. Uphold HQ, Inc*., 686 F. Supp. 3d 323)
- Commercial Code § 8507(b): transfers were "effective" per User Agreement § 3.7 (Ex. J1 at 7) D. Other Claims (pp. 19–20)
- No fiduciary duty owed (*Kurtz-Ahlers, LLC v. Bank of Am*., 48 Cal. App. 5th 952)
- Damages limited to value at time of loss; no lost-profits or consequential damages (Ex. J1 § 8.2)
- Attorneys' fees disallowed absent frivolous claims (Ex. J1 App. 5 § 1.7)

DECISION

Per the Scheduling Order entered on June 26, 2024, the parties agreed that the award shall provide concise written reasons for the decision pursuant to Consumer Rule R-43.

Facts that were adduced during the Evidentiary Hearing provide a record that is fertile with documentary evidence, verbal on oath witness and expert testimony, and expert reports.

The evidence presented in the evidentiary hearing established clear, credible and substantially unrebutted proof that:

- Respondent chose to select and partner with TaskUs as an outsourcing firm to provide customer support several years before 2024.
- Claimant's Coinbase account was the subject of a socially engineered cyberattack resulting in his account being taken over ("ATO") and depleted of $328,665.12 in cryptocurrencies between January 6-9, 2024, comprised of the following currencies 80.32821581 ETH ($191,469.93), 2.94674842 BTC ($134,685.32), 45.20641169 AVAX ($1,545.38), and 5,942.695564 GRT ($964.49).
- A TaskUs data breach was made known to Respondent by TaskUs in January of 2025 yet not reported to Claimant or other Coinbase customers until May of 2025.
- When the Respondent's announcement was made on May 15, 2025, it was delivered by its CEO Brian Armstrong who stated, *inter alia*, that
    - So first, any customers that were socially engineered as a result of this incident, we're going to reimburse them. (C22)
- Paul Bernardi- Head of Investigations on the Coinbase Trust and Safety Team, provided on oath testimony, which was in many instances noticeably evasive and neither forthcoming nor credible as exemplified generally throughout his testimony and more specifically by these portions of the transcripts. (Bernardi, Tr. 188:3-6 (Oct. 14, 2025), (Bernardi, Tr. 1000:8-7 (Oct. 16, 2025), (Bernardi, Tr. 1002-1003:24-3 (Oct. 16, 2025), (Bernardi, Tr. 1002:10-20 (Oct. 16, 2025) and (Bernardi, Tr. 1003:8-15 (Oct. 16, 2025)
    - When asked if there is any distinction between a social engineering incident of the type Armstrong was speaking of in this transcript and the one to which Claimant was subjected, Mr. Bernardi was (in the noticeable absence of any investigation to rely upon) unable to marshal facts to respond to this question nor could he identify a substantive distinction while acknowledging that Claimant was indeed the victim of social engineering. (Bernardi, Tr. 330:20-24 (Oct. 14, 2025)
    - It was clear from Mr. Bernardi's testimony that Respondent did not lift a finger to investigate the social engineering ATO that Claimant was subjected to between January 6-9, 2024.
    - With no investigative efforts taken by Respondent into the incident, Bernardi's testimony

further established quite noticeably that, as its Head of Investigations, he was unable to confirm or deny if Claimant's confidential account and personal information was compromised by and sold to others by TaskUs personnel.[1] As the custodian of Claimant's cryptocurrency account, Respondent -- without even conducting an investigation, of the type reasonably expected to be conducted under the circumstances, into the genesis and root cause of Claimant's ATO -- could not offer evidence to rebut that Claimant was the victim of the same type of TaskUs data breach handiwork that prompted Respondent's May 15, 2025 Armstrong PR announcement.

- Respondent prepared and issued to Claimant its "Notice of Data Breach" dated May 30, 2025, stating that his account information had been accessed by "a small number of individuals performing services for Coinbase" who may have then "shared it with a third party". The "Notice" (J-10)
- The Notice goes on to provide that the purloined information may have included Claimant's personal identifiers such as his social security numbers (last 4 digits), account numbers, bank account identifiers, account information including transaction history, account balance and transfers. (J-10)
- Claimant's testimony established that the information identified in the Notice is precisely the same information that the perpetrator(s) possessed and offered to him to gain his confidence that he/they was/were indeed Coinbase representative(s) as part of the ATO process he experienced. The record is devoid of any evidence that Claimant revealed his own private account information, was culpable, reckless, contributorily neglectful or otherwise acted or failed to act in a manner that contributed to or permitted this information to be leaked or compromised.
- Expert reports and testimony were offered by Jason Ghetian (J36) for Claimant and Steven McNew for Respondent (R8). In my opinion, these experts were skilled, uniquely qualified and offered extremely insightful and pointed testimony, which greatly assisted me in understanding the complexities of this dispute.

Jason Ghetian

In his expert report and testimony Mr. Ghetian opined

- Claimant was the victim of a data breach involving Coinbase's overseas contractors TaskUs, who were actively selling customer data to cybercriminals in exchange for bribes. When announcing the breach in May 2025, Coinbase noted that the cybercriminals wanted the data in order to impersonate Coinbase representatives for the purpose of stealing cryptocurrency. (Report at p.3)
- The attacker used social-engineering phone calls, criminal cyber infrastructure, and a Windows device inconsistent with Maini's history of Apple devices to gain unauthorized access. Coinbase permitted the attacker to maintain access using SMS verification, despite industry and National Institute of Standards and Technology (NIST) guidance that SMS is a weak factor unsuited for high-risk operations. Once inside, the attacker engaged in systematic account draining, liquidating twenty cryptocurrencies into USD using Advanced Retail Trade (a platform Maini had never accessed prior) and consolidating the funds into ETH for withdrawal. Coinbase's account-takeover (ATO) model failed to properly flag these transactions as anomalous when compared to A. Maini's usual Coinbase use, and rated four of the five transfers, including two over $100,000, as low risk. The stolen funds were laundered through ChangeNow, N.exchange, and RailGun, all of which are headquartered overseas making records hard to obtain. (Report at p.3)

[1] Despite Respondent's repeated, conspicuous and unpersuasive efforts to distant itself from TaskUs evident in its oft-repeated use of deflective language portraying itself as a victim rather than accepting responsibility as the party that invited TaskUs to access Claimant's and all other of its customers' private account information. It is undeniably evident from the record now at bar that Respondent determined years prior to Claimant's losses to choose, contract with and utilize TaskUs. A decision through which it then provided TaskUs personnel unfettered access to valuable and extremely private customer account information to provide customer support.

- Evidence further indicates that Maini's Yahoo email account was likely compromised and that insider data leaks, consistent with Coinbase's later disclosure of the TaskUs contractor breach, enabled the attacker to convincingly impersonate Coinbase. Coinbase's reliance on passive blog posts left customers like Maini without timely warnings about relevant threats, and its automated holds proved insufficient without manual review. (Report at p.3)
- The information the attacker had about Dr. Maini's account could not have been obtained without insider information and that based on his research "there's no way that this cyber actor would have had the information he did on Dr. Maini, absent obtaining it through an insider". (Ghetian, Tr. 686:11-15 and 687:8-12 (Oct. 15, 2025). Mr. Ghetian added that Dr. Maini was a confirmed victim of the TaskUs data breach. (Ghetian, Tr. 687:14-17 (Oct. 15, 2025). He also observed that Coinbase chose not to tell Dr. Maini what information was illegally given away and *didn't disclose when* Dr. Maini's information was illegally accessed or given away or sold. (Ghetian, Tr. 759:1-10 (Oct. 15, 2025). Mr. Ghetian testified that the attack on Dr. Maini is consistent with other victims that he knows to be victims of the TaskUs breach, and is consistent with the modus operandi, as described by Coinbase in its letters to the victims of the TaskUs breach warning them of social engineering scams. (Ghetian, Tr. 759:19- 25 (Oct. 15, 2025).
- When asked if the risk that was presented to Coinbase customers from the TaskUs incident predated the discovery of that risk in December 2024, Mr. Ghetian confirmed that the risk had been going on for years. (Ghetian, Tr. 694-695:11-1 (Oct 15, 2025). Mr. Ghetian further testified that he has viewed Telegram chat forums that disclose Coinbase employees selling data well before the TaskUs breach was announced. (Ghetian, Tr. 762:1-5 (Oct. 15, 2025). Mr. Ghetian also acknowledged that the class action complaint filed in the Southern District of New York alleged that TaskUs had been providing overseas customer support to Coinbase since approximately 2019 and that TaskUs terminated as many as 300 employees following an internal investigation into the breach. (Ghetian, Tr. 806-807:12-7 (Oct. 15, 2025)

Steven McNew

In his expert report and testimony, Mr. McNew opined that:

- In the 50-60 instances in which he has actively investigated and determined causation for ATOs and impersonation schemes in the crypto industry, he has observed that 95% or more exhibit an email account being taken over or infiltrated as a trigger or part of the ATO scheme. (McNew, Tr. 1133 – 1134 (Oct. 16, 2025).
- In reviewing transaction logs and IRIS reporting issued by Respondent, he agreed that the template description of notifications assessing risk by using the words "risky' or "risk" is evidence that a risk is being encountered which is what triggers Respondent to deliver an email or send a push notification to Claimant. (McNew Report pp. 21-22, McNew Tr. 1137:6-24 (Oct. 16, 2025).
- In all instances in which this log shows on January 9, 2024, that emails are being sent to Claimant by Respondent concerning ongoing account conduct that is characterized by Respondent as "risky", we have cause for concern whether Claimant is getting the emails, we certainly know that the bad actor is getting those emails. (McNew Report pp. 21-22, McNew Tr. 1139:3-14 (Oct. 16, 2025).
- With Respondent having elected to not engage in an investigation into the causes of Claimant's 2024 ATO it had and offered no substantive explanation, leading me to question Mr. McNew as follows: "Q: So if in nine and a half out of 10 cases that happens, then you would agree with me, would you not, that a

canyon of emails alerting the customer to transactions affecting their account is, you know, going to, in nine and a half out of 10 cases, arguably be ineffectual because they're not reaching the intended target, right? A: Completely agree.". (McNew Report pp. 21-22, McNew Tr. 1135:13-21 (Oct. 16, 2025).

- With it being established that 95% or more of ATO's like the one resulting in Claimant's losses here, are being perpetrated by an email account being infiltrated, it was conversely said by Mr. McNew to be true that 5% or less of such instances are the result of a phone being overtaken, hacked or infiltrated. (McNew Tr. 1147-48:19-10 (Oct. 16, 2025).
- In questioning Mr. McNew to ascertain why Respondent's communication efforts in such instances should not rely more heavily upon phone notifications (which exhibits a 5% or less chance of causing an ATO) than on emails which feature a 95% more perilous means of communicating in alerting its customers that a "risky" transaction may be afoot, I asked him: "Q: So any other reasons you would think that this, you know, 5 percent risk would not be more attractive to Coinbase and other custodians of crypto? A: Well, I guess I'm not entirely sure -- well, I don't want to say I don't agree.". (McNew Tr. 1149:16-22 (Oct. 16, 2025).

Gross Negligence

On the claim of gross negligence, I find for the Claimant and against the Respondent.

Under California common law, gross negligence is based upon the traditional elements of negligence: duty, breach, causation, and damages. *Chavez v. 24 Hour Fitness USA, Inc.*, 238 Cal. App. 4th 632, 640 (2015). Gross negligence has long been defined as either a "want of even scant care" or "an extreme departure from the ordinary standard of conduct". *City of Santa Barbara v. Superior Court*, 41 Cal. 4th 747, 749, (2007). Here, in acting as a custodian of Claimant's fungible cryptocurrencies, Respondent is bound by a legal duty to take reasonable precautions to protect the same assets over which it acted as custodian. This conclusion is self-evident from sum-total of the considerations relevant to the transactional relationship existing between the parties. Respondent deviated from the normal standard of conduct as a custodian in its initial election to offer and share highly confidential customer account information with TaskUs -- which it possessed as the "for hire" custodian of Dr. Maini's crypto holdings – as that election proved to be the causal link that set in motion Claimant's losses and a vector for the fraud which ensued. Whenever a party to an asset based custodial relationship is entrusted with their customers' confidential and private account information *including account balances* and account access information, it has a clear and present duty to exercise due care in those it entrusts with this same information.

On May 30, 2025, Respondent issued its "Notice of Data Breach" to Claimant to alert him that his private personal identifiers such as passwords, private keys, social security numbers, account numbers, bank account identifiers, email addresses and related account information were compromised in the TaskUs scandal and may have been disclosed to a third party. (J10). In May of 2025 Respondent's CEO stated: "So first, any customers that were socially engineered as a result of this incident, we're going to reimburse them." (C22). In publicly offering to reimburse its customers for losses resulting from Respondent's selection and use of TaskUs and then failing to lift a finger to investigate the root cause of Dr. Maini's January 9, 2024 losses, Respondent not only set motion the cause for this ATO, but it also then rendered Armstrong's promise disingenuous and in so doing, acted with a want of even scant care. Respondent's SOP evidence an approach in which it simply ignored that less than 5% of ATO's result from a customer's cell phone being hacked or infiltrated in favor of using email notifications to alert its customers when their assets are at risk when 95% or more of these scams are perpetrated through an email account being compromised or infiltrated, as occurred here. When asked to explain why, in the midst of a socially engineered ATO, Respondent relied so heavily on email notifications when it is highly unlikely those emails are even being seen by their customers, no cogent explanation was offered.

In whatever vetting and decision-making process Respondent relied upon to select and trust its own employees and TaskUs personnel with this same highly confidential information, a factual conclusion emerges as inescapable;

Respondent utterly failed in its duty to protect and maintain as private, Claimant's and many other of its own customers' confidential account information. In viewing the progression of incidents that culminated in Claimant's losses on January 9, 2024, it is apparent that providing this information (*particularly customer account balances*) enabled TaskUs personnel and its own employees with the unique ability to select and target only those higher value accounts as those being most worthy of an ATO campaign. Once available, this information in turn monetized and created a price or trade value for these same customers' account information inviting a transactional black market to form in which the thievery and sale of this same information became commonplace. But for Respondent's deviation from an acceptable standard of conduct (the exercise of reasonable caution) those entrusted by Respondent with this incredibly sensitive account information would not likely have had the opportunities that Respondent handed them. It appears that Respondent didn't think through the likely ramifications and the ensuing ATO risks caused by its election to entrust TaskUs and its employees with its own customers' confidential account and account balance information. Respondent exhibited reckless decision making and itself spawned an illicit marketplace and clearinghouse for the pricing, acquisition and sale of the same confidential customer information it was duty bound to protect. To me it is evident that Respondent's poor decision making was the catalyst for all the social engineering ATOs which ensued.

Breach of Contract and Implied Covenant of Good Faith, Breach of Fiduciary Duty, Fraudulent and Negligent Misrepresentation

On the Breach of Contract and Implied Covenant of Good Faith, Breach of Fiduciary Duty, Fraudulent and Negligent Misrepresentation claims, I find for the Claimant and against the Respondent.

Breach of Contract and Implied Covenant of Good Faith

Included among the terms of the parties' User Agreement, Section 5 (3) of Coinbase's Privacy Policy provides:

> We process your personal information in order to help detect, prevent, and mitigate fraud and abuse of our services and to protect you against account compromise or funds loss. (J1)

Section 5(8) states:

> We process your personal information in order to enhance security, monitor and verify identity or service access, combat spam or other malware or security risks and to comply with applicable security laws and regulations. The threat landscape on the internet is constantly evolving, which makes it more important than ever that we have accurate and up-to-date information about your use of our Services. Without processing your personal information, we may not be able to ensure the security of our Services. (J1)

In Section 10 of the Privacy Policy Coinbase went on to represent that it would:

> …store [Dr. Maini's] personal information securely throughout the life of [his] CB account.

Under California common law, a breach of contract claim requires the existence of a contract, performance or excuse for nonperformance, breach, and resulting damages therefrom. *Wall Street Network Ltd. v. New York Times Co*., 164 Cal. App. 4th 1171, 1178 (2nd Dist. 2008). Respondent's Privacy Policy is incorporated by reference into the User Agreement, making it part of the contract. *In re Facebook, Inc. Consumer Priv. User Profile Litig.,* 402 F.Supp.3d 767, 791 (N.D. Cal. 2019) ("California law makes it quite easy to incorporate a document by reference.") Furthermore, "the law implies in every contract a covenant of good faith and fair dealing." *Fleet v. Bank of America N.A.,* 229 Cal. App. 4th 1403 (2014).

Respondent breached the provisions of this Privacy Policy by allowing Claimant's personal account information to be freely accessible by personnel it recklessly selected when it outsourced customer support who then sold the same information to third parties. Through this data breach, as noted above, there is ample evidence in this record to establish that Claimant's private account information was sold by a TaskUs contractor to a cybercriminal who then used Claimant's information for a social engineering scam against Claimant. Respondent breached its User Agreement by failing to properly secure and protect Claimant's personal information and in turn his Coinbase

account. These incidents of breach then allowed Claimant's email account and later his Coinbase account to be taken over by an unauthorized third-party and pillaged. In my view the ATO experienced by Claimant was proximately caused by the same risks visited upon him due to Respondent's acts and omissions in improvidently selecting, retaining and cavalierly entrusting TaskUs personnel with highly confidential account information complete with his account balance which proved to be a disastrous choice for the Claimant and many more similarly affected Coinbase customers. Just as night follows day, Respondent's incidents of breach have also violated its implied duty of good faith as it repeatedly was vested with discretion under the User Agreement which it failed to exercise reasonably but instead indiscriminately and recklessly in its selection and use of TaskUs and its determination of what account information it would share, a choice which proximately caused harm to Claimant.

Breach of Fiduciary Duty

In its role as a custodian of its customers' assets, Respondent agreed to act as Claimant's agent when buying and selling supported cryptocurrencies on its platform. Under California law "the relations between principal and agent, like those of beneficiary and trustee, are fiduciary in character." *Kinert v. Wright*, 81 Cal. App. 2d 919, 925 (1947). Further, "[a]n agent who violates his duty to use reasonable care, skill and diligence is liable for any losses which his principal may sustain as the result of his negligence or breach of duty." *Timmsen v. Forest E. Olson, Inc*., 6 Cal. App. 3d 860, 871 (1970). Respondent breached the fiduciary duties it owed to Claimant as his custodial agent when it set in motion *via* TaskUs, the opportunity of nefarious third-party cybercriminals to access private account information used to target Claimant. As noted above, it was Respondent's choice to share customer account balances with TaskUs and that choice triggered thousands of ATOs as it permitted bad actors to identify and target only higher value accounts, a distinction that then enabled bad actors to determine the price for the sale and purchase of ill-gotten information. There was no evidence offered by Respondent to explain why including account balances was necessary as part of the information it shared with TaskUs and its employees. Through this vector the cybercriminal(s) then executed the liquidation of nearly all of Claimant's cryptocurrency holdings.

It also bears mentioning that once the criminal trade transactions began on Claimant's account on January 9, 2024, they were permitted to be consummated by Respondent despite the many risk warning signs detailed in the record now at bar. While Respondent knew or should have known that at all times material during this incident, over 95% of ATOs on its platform were occurring due to a takeover of a customer's email account. This same conclusion was arrived at by Mr. McNew, and yet Respondent still blindly persisted in relying upon *emailing* Claimant with warnings of questionable trading activity when it appears clear that none of these emails were being received by him. If charged with having the same knowledge that Mr. McNew testified to, Respondent also knows or should have known that 5% or less of ATOs occurring on its platform are based on a hacked or infiltrated phone. Although equipped to change its approach based on these security facts, it defies reason that Respondent never once phoned or texted Claimant to communicate warnings which if done would likely have stopped the criminal transactions from being consummated. Here instead of being proactive and using a more secure means of communicating with Claimant, Respondent ignored and breached its fiduciary duties on multiple levels, green lighting all of the transactions for which it collected transaction fees as Claimant's cryptocurrencies were jettisoned to unknown wallets.

Despite Claimant notifying Coinbase as soon as he knew about the unauthorized transactions, as Coinbase instructs its customers to do elsewhere in its User Agreement, Coinbase made no efforts to act on his concerns, investigate the root causes for his ATO or to offer an explanation identifying why it did not reimburse Dr. Maini. Based on the facts at bar, these failures were inexcusable since Respondent acknowledged (i) that his account and personal information was accessed in a TaskUs data breach and (ii) after Mr. Armstrong publicly announced that Respondent would reimburse those victimized by its election to share confidential account information as it outsourced its customer service duties to TaskUs. Through this broadly publicized statement Respondent convincingly advertised that it made a mistake and would reimburse and not forsake the customers whom it exposed to socially engineered ATOs. This announcement was made to signal that as a company who values and invites customer trust, Respondent would honor the promises made by its CEO, and yet once the camaras were turned off and the PR messaging campaign ended, it chose not to keep these same promises, as was evident in its dealings with Claimant. This about-face not only violates Respondent's User Agreement, it evidences a far more harmful motive to engage in what appeared to be a bait and switch scheme to offer virtuous platitudes of customer reimbursements before the camera made to regain the confidence of its customers but then renege on the same PR promises offered by its CEO. Despite these platitudes, judging from this dispute, Respondent has elected a strategy to disavow Armstrong's promise by fighting

(and not honoring) legitimate reimbursement claims while doing its best to keep this inexplicable approach out of the public eye. As a result of Coinbase's failure to act with reasonable care, skill and diligence, it has breached its fiduciary duties to Claimant as its principal and is liable to Claimant for all resultant damages of its conduct.

Fraudulent and Negligent Misrepresentation

Respondent knowingly or recklessly misrepresented its security practices, its role as a privacy concerned and careful custodian of account information and assets (which it was not), its vow to reimburse those customers victimized by the TaskUs data breaches it caused, its compliance posture and its Privacy Policy. For the reasons set out above and elsewhere in this record of proceedings, these misrepresentations directly caused Claimant's loss. Fraud occurs when a misrepresentation is made and then includes a concealment or nondisclosure, the actor has knowledge of the falsity of the representation and intends to induce reliance on the misrepresentation and the victim justifiably relies on the statements as being truthful and incurs resulting damages. *Small v. Fritz Companies, Inc*. 30 Cal.4th 167, 173 (2003). A cause of action for negligent misrepresentation is identical to fraud, *sans* any requirement of intent to induce reliance. (*Id.*) In both causes of action, to prevail the victim must plead and prove that he or she actually relied on the misrepresentation. *Mirkin v. Wasserman* 5 Cal.4th 1082, 1088–1089 & fn. 2 (1993). The evidence established that the Claimant here has satisfied its proof burden and established evidence to support my finding that he has prevailed on both his fraudulent and negligent misrepresentation claims.

Violation of California False Advertising Law, Violation of Cal. UCC § 8507(b) & Violation of the Electronic Funds Transfer Act (15 U.S.C. § 1693 et seq.)

On the California False Advertising Law and the UCC claims I find for Claimant while on the EFTA claim I find for the Respondent.

California False Advertising Law

Respondent's Privacy Policy and marketing materials describe the platform as offering "bank-level security," "industry leading security," that it has the "most secure and multifaceted risk management programs to protect customer assets," and "that it is constantly working to protect" customer from "emerging threats". Additionally, when Respondent presented witnesses it appeared remarkable that none could identify the date that it initially selected and utilized TaskUs and in turn provided its personnel with sensitive and highly confidential customer account information. While Claimant's expert estimated the date to be 2019 some reports reveal this may have occurred as early as 2017. When facing a fact question so crucial to Respondent's defense, it is incumbent upon the defending party to provide factual evidence in the form of documents and witness testimony. Here Respondent repeatedly failed to provide such factual support for its defenses and the witness it presented as the Head of Investigations on the Coinbase Trust and Safety Team appeared to have selective amnesia as he was evasive and not forthcoming, having no recollection of critical facts that may if revealed be harmful to its defenses.

When news of the TaskUs data breach was finally revealed publicly by Respondent's CEO in May of 2025, he clearly offered to reimburse those of its customers victimized by the incident. Instead of explaining the date it initially entrusted TaskUs and accepting accountability for ATO's occurring for reasons which would point to TaskUs as the causal connection, Respondent chose to disavow the notion that any losses, *whenever* they occurred and which were otherwise not shown to be the fault of the customer, were more likely than not caused due to TaskUs personnel accessing and selling valuable confidential account information to scammers. As was evident from the evidence adduced at trial, Respondent then elected another flawed strategy to refuse to undertake any investigation into any earlier occurring losses, just as it did when faced with Claimant's losses here. Respondent's offer to reimburse the ATO victims for losses occurring in late 2024 and early 2025 due to TaskUs conduct, while not similarly offering to include those who suffered the same TaskUs caused losses *whenever* they occurred, is senselessly predicated upon a difference without a distinction as all such losses should likewise be reimbursed by it. Indeed, if losses occurred to its customers *before* it learned in late 2024 and early 2025 of the data breaches due to TaskUs being given access to and selling Claimant's account information, then the rationale for reimbursing him for the same losses which occurred earlier, is identical to the reason for reimbursing any of its customers as was stated by Armstrong in his May 2025 PR announcement.

California law prohibits "any unlawful, unfair or fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising," and any act prohibited by the false advertising law. (Bus. & Prof. Code, § 17200.) *Chapman*

v. Skype, Inc., 220 Cal. App. 4th 217, 228 (2nd Dist. 2013). California false advertising law generally prohibits advertising that contains "any statement … which is untrue or misleading, and which is known, or … should be known, to be untrue or misleading … ." (Bus. & Prof. Code, § 17500.). Id. The remedies available to a private plaintiff under the UCL and the false advertising law include injunctive relief and restitution. Bus. & Prof. Code, §§ 17203, 17535; *Kasky v. Nike, Inc*. 27 Cal.4th 939, 950 (2002). To state a claim under either the UCL or the false advertising law, based on false advertising or promotional practices, 'it is necessary only to show that "members of the public are likely to be deceived."' *Kasky, supra*, 27 Cal.4th at 951. This is determined by considering a reasonable consumer who is neither the most vigilant and suspicious of advertising claims nor the most unwary and unsophisticated but instead is "the ordinary consumer within the target population." *Lavie v. Procter & Gamble Co*. 105 Cal.App.4th 496, 509–510 (2003). "'Likely to deceive' implies more than a mere possibility that the advertisement might conceivably be misunderstood by some few consumers viewing it in an unreasonable manner. Rather, the phrase indicates that the ad is such that it is probable that a significant portion of the general consuming public or of targeted consumers, acting reasonably in the circumstances, could be misled." (*Id*. at 508.) Claimant and Respondent submitted substantial evidence that the latter touts its Privacy Policy, security and investigative measures, aggressively promotes its use of machine learning to actually protect its customers from fraud. Given the genesis and nature of the attack against Claimant, contrary to its advertising materials and PR representations, there are severe issues plaguing Coinbase's security apparatus which it knows of or should in the exercise of reasonable caution should know of, including:

- that it does not investigate losses like those suffered by Claimant
- it does not respond in kind to high threat levels on customer accounts or conduct any human review when the machine learning models are warning it of high-risk transactions
- it does not refrain from emailing account alerts during high-risk transactions despite knowing that almost all ATOs are the result of email address takeovers
- it does not use customer phones to provide the same alerts it emails its customers in high-risk moments while knowing that less than 5% of ATOs occur through phone hacks
- it does not adhere to its own Privacy Policy and instead entrusted TaskUs for many years with highly sensitive customer account information including account balances, all so that it could outsource customer support.

Under the totality of the circumstances, Respondent has repeatedly made factual representations that have proven to be materially false when made, and which induced Claimant's initial and ongoing reliance. As such for reasons set out above, I find that Respondent has engaged in unlawful, unfair or fraudulent business acts and practices and unfair, deceptive, untrue or misleading advertising in a manner that violates California's false advertising law.

Violation of California Uniform Commercial Code § 8507(b)

I find that Respondent acted on "ineffective entitlement orders." Under § 8507(b), it was required to reestablish Claimant's security entitlement or credit his account as he was always the true and rightful owner of the cryptocurrency in his account. As such, Claimant qualifies as an entitlement holder with respect to that "financial asset" under California's UCC statutory scheme. California UCC § 8507(b) provides a statutory private right of action against securities intermediaries, like Respondent, which executed "ineffective entitlement orders" here which then provides that:

> If a securities intermediary transfers a financial asset pursuant to an ineffective entitlement order, the securities intermediary shall reestablish a security entitlement in favor of the person entitled to it and pay or credit any payments or distributions that the person did not receive as a result of the wrongful transfer. If the securities intermediary does not reestablish a security entitlement, the securities intermediary is liable to the entitlement holder for damages." Cal. U Com. Code §8507(b).

Coinbase contractually accepted the responsibility to be held to the standard of a securities intermediary under the California UCC, and it unlawfully failed to reestablish Claimant's security entitlement or credit his account following the loss incidents of January 9, 2024.

Violation of the Electronic Funds Transfer Act (15 U.S.C. § 1693 et seq.)
EFTA covers only transfers from "accounts" "established primarily for personal, family, or household purposes. 15 U.S.C. §§ 1693a(2), 1693g(a). Courts interpreting EFTA and its parallel provisions in the Truth in Lending Act and Bankruptcy Code have repeatedly held that "personal, family, or household purposes" excludes investment accounts and those established with other "profit" motives. (EFTA); see also *Cobb v. Monarch Fin. Corp*., 913 F. Supp. 1164, 1174-75 (N.D. Ill. 1995) (EFTA*); Pfeffer v. HSA Retail, Inc*., 2012 WL 1910034, at *4 (W.D. Tex. May 24, 2012) (EFTA); *In re Booth*, 858 F.2d 1051, 1054- 55 & n.9 (5th Cir. 1988) (summarizing TILA cases); *In re Runski*, 102 F.3d 744, 746- 47 (4th Cir. 1996) (bankruptcy). Here, consistent with what Claimant told Respondent when he opened his account, Ex. 18 R7, Claimant testified that he used his Coinbase account for "investment purposes." Tr. 340:5–8, Tr. 404:16 (his account was for "investments"). And Claimant's account activity is consistent with a user attempting to maximize profit from crypto investing. Tr. 230:10–13. As such, Claimant has failed to provide evidence sufficient to prevail on his EFTA claims and Respondent has provided well supported defenses sufficient to find in its favor and against Claimant.

AWARD

Based upon the foregoing I find that Claimant is entitled to damages equal to $329,665.12 reflecting the value of all of his cryptocurrencies/property which were unlawfully taken from him on January 9, 2024. Respondent is ordered to pay Claimant (through his legal counsel) this sum, together the with other amounts being awarded as detailed below, within twenty-one (21) days of the date of this order, and the parties are directed to confer and determine a suitable method for effectuating this payment.

Additionally I find that based upon Respondent's conduct in the handling of these claims, Claimant should recover an additional sum in the amount of $150,000 in U.S. dollars to compensate him for the loss of use of his own funds and in recompense for Respondent's actions taken and ignored in connection with his ATO and ensuing claims. This award is appropriate insofar as Claimant was never asked and never consented to the sharing of his information by Respondent which resulted in the sale of his private account and personal information which still to this day may result in additional attacks on his business and personal accounts elsewhere. Allowing Claimant's confidential account information to be purloined through the TaskUs-premised security lapses and its ensuing promise to reimburse such losses which it refused to do here when asked by Claimant, followed by its refusal to investigate the root causes for his losses were in this Arbitrator's opinion clearly the result of its improvident selection, oversharing of account information and use of TaskUs. It is almost as if Respondent's refusal to investigate this incident is being relied upon by it to evade accountability, which are badges that no reputable asset custodian should want to be associated with much less impose upon its customers.

While Claimant's attorneys have stated in the Post Trial Brief that their fee request is premised upon a 29% contingency arrangement, they also stated their fees were detailed in his "Attorney's Fee Declaration filed in this arbitration". As there appeared to be no Attorneys' Fee Declaration of record, accepting that a contingency exists as presented by Claimant, I further find the Respondent owes to Claimant the sum of $95,602.85 as for its attorneys' fees calculated based only upon the $329,665.12 portion of the award. As for an award of costs, Claimant included as Exhibit 1 to its Post Trial Brief its "CLIENT LEDGER" detailing his costs totaling $41,947.29. As such, I am entering a contingent award of costs in the amount of $41,947.29 on the condition that Claimant promptly provide to AAA applicable invoices identifying these same costs which it asserts it is obligated to pay together with any proofs of payment in his possession. I reserve the right to deduct from this award any cost items which are not supported through Claimant's submission.

Finally I deny Respondent's request to impose confidentiality designations as requested by it on October 29, 2025 as those requests are untimely, overbroad and would permit it to improperly engage in conduct that on the one hand seeks to elicit favorable testimony on direct examination but then on the other asks to secrete harmful testimony on cross examination and testimony offered in response to my own questions. This determination applies to both the Protective Order entered in this matter and the User Agreement confidentiality restrictions insofar as California law is clear that confidentiality agreements and protective orders cannot be used as both a sword and a shield which is plainly what Respondent seeks to accomplish on the heels of disavowing and breaching so many of its own contractual and common law duties in its dealings with this Claimant. *Ford v. City of Los Angeles*, 47 Cal. App. 5th

277, 286 (2020).

The legal basis for my findings and this award is premised upon the factual record of proceedings and all exhibits presented by the parties with the stated intent to award relief that I have deemed appropriate based on broad principles of justice and equity, . even if such relief would not have been allowed by a court or were contrary to substantive law or the terms of the parties' User Agreement.

The administrative fees of the American Arbitration Association totaling shall be borne as incurred, and the compensation of the arbitrator shall be borne as incurred.

This Final Award is in full settlement of all claims submitted to this arbitration. All claims not expressly granted herein are hereby denied.

12/11/2025
Date


Steven Michael Ruffalo, Arbitrator

I, Steven Michael Ruffalo, do hereby affirm upon my oath as arbitrator that I am the individual described in and who executed this instrument, which is my Award.

12/11/2025
Date


Steven Michael Ruffalo, Arbitrator